



Palo Alto Networks®

Guía del administrador de WildFire

Versión 6.0

Información de contacto

Sede de la empresa:

Palo Alto Networks

4401 Great America Parkway

Santa Clara, CA 95054

http://www.paloaltonetworks.com/contact/contact/

Acerca de esta guía

Esta guía describe las tareas administrativas necesarias para utilizar y mantener la función Palo Alto Networks WildFire. Los temas tratados incluyen información de licencias, la configuración de cortafuegos para reenviar archivos para su inspección, la visualización de informes y cómo configurar y gestionar el Dispositivo WF-500 WildFire.

Consulte las siguientes fuentes para obtener más información:

- Guía del administrador de Palo Alto Networks: Ofrece información sobre capacidades adicionales e instrucciones sobre la configuración de las funciones del cortafuegos.
- https://live.paloaltonetworks.com: Permite acceder a la base de conocimientos, la documentación al completo, foros de debate y vídeos.
- https://support.paloaltonetworks.com: Aquí podrá contactar con el servicio de asistencia técnica, informarse sobre los programas de asistencia y gestionar su cuenta o sus dispositivos.

Para enviar sus comentarios sobre la documentación, diríjase a:

documentation@paloaltonetoworks.com

Guía del administrador

www.paloaltonetworks.com

Número de pieza 810-000216-00A

Contenido

Descripción general de WildFire 1

¿Cómo funciona WildFire? 2

¿Qué tipos de archivos puede analizar WildFire? 5

¿Cómo puedo ver informes en archivos analizados por WildFire? 6

¿Qué acciones debo tomar después de que se detecte malware? 7

¿Qué implementaciones están disponibles? 8

¿Cuántos archivos puede reenviar el cortafuegos a WildFire? 10

¿Cuáles son las ventajas de la suscripción de WildFire? 11

¿Desde dónde puedo acceder a un archivo de muestra de malware para su prueba? 13

Análisis de archivo de WF-500. 15

Acerca del dispositivo WF-500 WildFire. 16

Configuración del dispositivo WF-500 WildFire 17

- Antes de comenzar 17
- Realización de la configuración inicial de WF-500 18
- Verificación de la configuración del dispositivo WF-500 WildFire 22
- Configuración de interfaz de la máquina virtual 25

Reenvío de archivos a un dispositivo WF-500 WildFire 30

- Recomendaciones para actualizaciones dinámicas 33
- Verificación de WildFire al reenviar a un dispositivo de WildFire. 34

Actualización del software del dispositivo WF-500 WildFire. 38

Análisis de archivo de la nube de WildFire 41

Envío de archivos a la nube de WildFire. 42

Recomendaciones para actualizaciones dinámicas 46

Verificación de WildFire al reenviar a la nube de WildFire 47

Carga de archivos en el portal de la nube de WildFire 51

Carga de archivos y consulta de WildFire mediante la API de WildFire 53

- Acerca de las suscripciones a WildFire y claves API. 53
- ¿Cómo usar la API de WildFire? 53
- Métodos de envío de archivos de la API de WildFire. 53
- Consulta de un informe PDF o XML de WildFire 55
- Uso de la API para recuperar un archivo de prueba de malware de muestra 56

Elaboración de informes de WildFire 57

Acerca de los logs de WildFire. 58

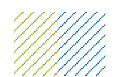
Supervisión de envíos con el portal de WildFire. 60

- Personalización de la configuración del portal de WildFire 60

Cuentas de usuario del portal de WildFire 62
Adición de cuentas de usuario de WildFire. 62
Visualización de informes de WildFire 64
¿Qué contienen los informes de WildFire? 65
Configuración de alertas para el malware detectado 68
WildFire en acción 71

Referencia de la CLI del software del dispositivo WildFire 77

Acerca del software del dispositivo WildFire 78
Acerca de la estructura de la CLI del software del dispositivo WildFire 78
Acceso a la CLI 79
Establecimiento de una conexión directa con la consola 79
Establecimiento de una conexión de SSH 79
Uso de los comandos de la CLI del software del dispositivo WildFire 79
Modos de comando de la CLI 85
Acerca del modo de configuración 85
Acerca del modo de operación 89
Establecimiento del formato de salida para comandos de configuración 89
Comandos del modo de configuración 90
interfaz vm 93
wildfire 94
Comandos del modo de operación 96
test wildfire registration 117
set wildfire portal-admin 118
raid 119
show wildfire 120
show system raid 124



Descripción general de WildFire

El malware moderno es el eje de la mayoría de los ataques a la red más sofisticados de la actualidad, y cada vez se personaliza más para burlar las soluciones de seguridad tradicionales. Palo Alto Networks ha desarrollado un enfoque integrado que se encarga de todo el ciclo de vida del malware, lo que incluye la prevención de infecciones, la identificación de malware de día cero (es decir, malware que no han identificado anteriormente otros proveedores de antivirus) o malware específico (dirigido a un sector o corporación concretos), así como la localización y eliminación de infecciones activas.

El motor de WildFire de Palo Alto Networks expone el malware específico y de día cero mediante la observación directa en un entorno virtual en el sistema WildFire. La funcionalidad WildFire hace, además, un uso extensivo de la tecnología App-ID de Palo Alto Networks identificando las transferencias de archivos en todas las aplicaciones, no solo en los archivos adjuntos del correo electrónico o en las descargas de archivos del explorador.

Las principales ventajas de la funcionalidad WildFire de Palo Alto Networks son la detección de malware de día cero y generar rápidamente firmas para ofrecer protección frente a futuras infecciones de todo el malware que detecte. El cortafuegos proporciona alertas instantáneas en cualquier momento en que se detecte malware en su red mediante el envío de alertas de correo electrónico, alertas de Syslog o traps SNMP. Esto le permite identificar rápidamente qué usuario descargó el malware y eliminarlo antes de que cause mayores daños o se propague a otros usuarios. Además, cada firma generada por WildFire se propaga automáticamente a todos los cortafuegos de Palo Alto Networks protegidos con las suscripciones a Threat Prevention o WildFire, que ofrecen protección automatizada frente a malware incluso si no se ha detectado dentro de la red.

Los siguientes temas describen WildFire y cómo integrarlo en su entorno:

- ¿Cómo funciona WildFire?
- ¿Qué tipos de archivos puede analizar WildFire?
- ¿Cómo puedo ver informes en archivos analizados por WildFire?
- ¿Qué acciones debo tomar después de que se detecte malware?
- ¿Qué implementaciones están disponibles?
- ¿Cuántos archivos puede reenviar el cortafuegos a WildFire?
- ¿Cuáles son las ventajas de la suscripción de WildFire?
- ¿Desde dónde puedo acceder a un archivo de muestra de malware para su prueba?

¿Cómo funciona WildFire?

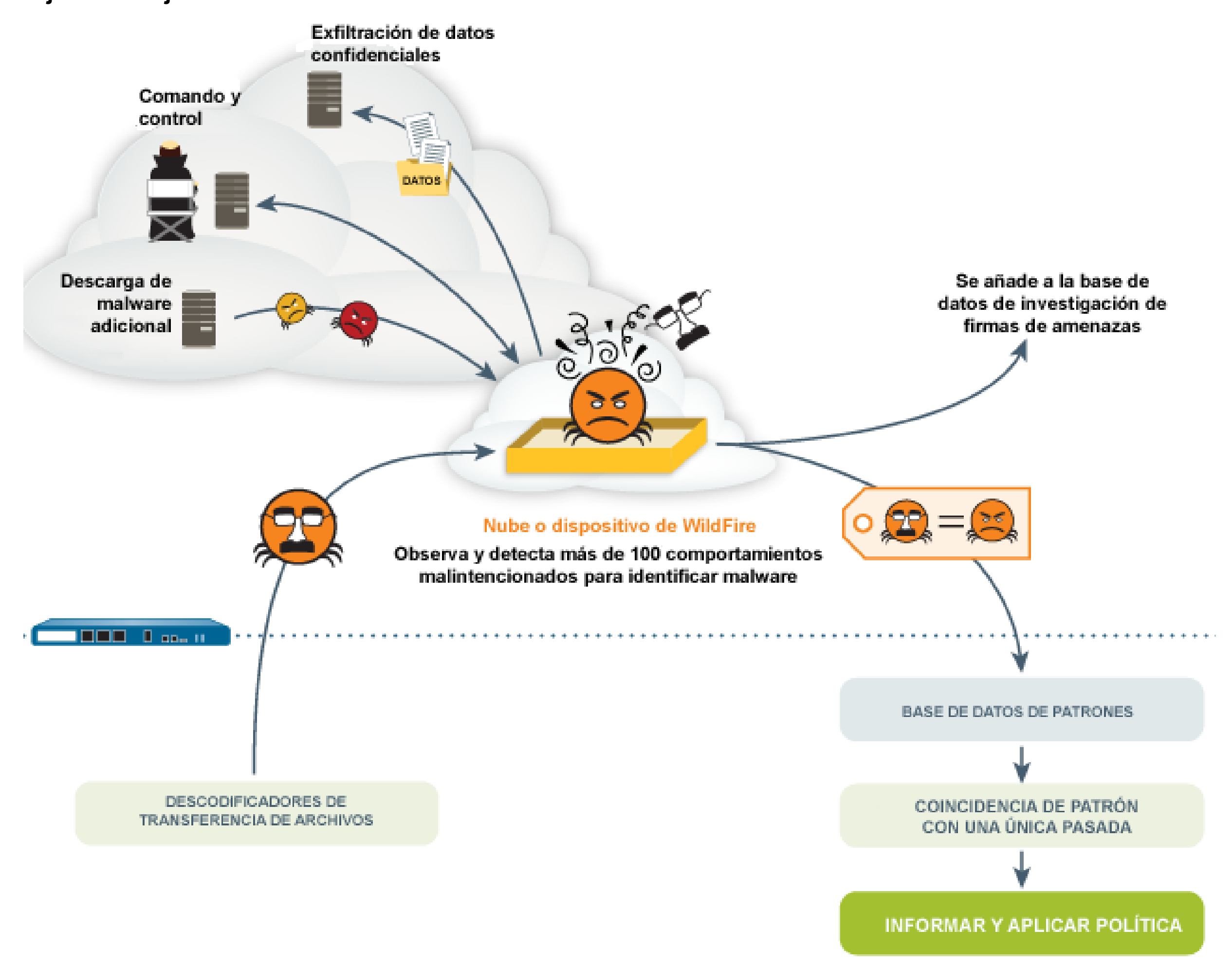
WildFire amplía las capacidades de los cortafuegos de próxima generación de Palo Alto Networks para identificar y bloquear el malware de destino y desconocido. Con esta solución integrada, configura el cortafuegos con un perfil de bloqueo de archivos que indica al cortafuegos que debe reenviar automáticamente los tipos de archivos que suelen verse comprometidos a WildFire y, a continuación, adjuntar el perfil a reglas de política de seguridad para tener un control detallado sobre las condiciones en las que los archivos se envían a WildFire. Siempre que se transfiere un archivo mediante una sesión que coincida con una regla de política de seguridad con un perfil de reenvío, el cortafuegos comprueba con WildFire si el archivo es nuevo. Si el archivo es nuevo, el cortafuegos lo reenvía automáticamente a WildFire, incluso si este se encontraba en un archivo ZIP o en HTTP comprimido. El cortafuegos también se puede configurar para que reenvíe archivos situados dentro de sesiones SSL descifradas.

WildFire ejecuta los archivos sospechosos que recibe en un entorno virtual y observa su comportamiento para determinar si muestran signos de comportamientos malintencionados, como cambios en la configuración de seguridad del explorador, introducción de código en otros procesos, modificación de archivos en las carpetas del sistema de Windows o dominios a los que la muestra ha intentado acceder. Cuando el motor de WildFire completa el análisis, genera un informe experto detallado que resume los comportamientos observados y asigna un veredicto para indicar si se trata de malware o no. Para los archivos que se determina que son malintencionados, WildFire genera automáticamente una firma basada en la carga útil de malware de la muestra y comprueba su precisión y seguridad. Dado que el malware evoluciona rápidamente, las firmas que genera WildFire cubrirán diversas variantes de este. La nueva firma se distribuye entonces en 30-60 minutos a todos los cortafuegos de Palo Alto Networks con una suscripción de WildFire, o el día siguiente como parte de la actualización del antivirus para los cortafuegos que solo tienen una suscripción de Threat Prevention.

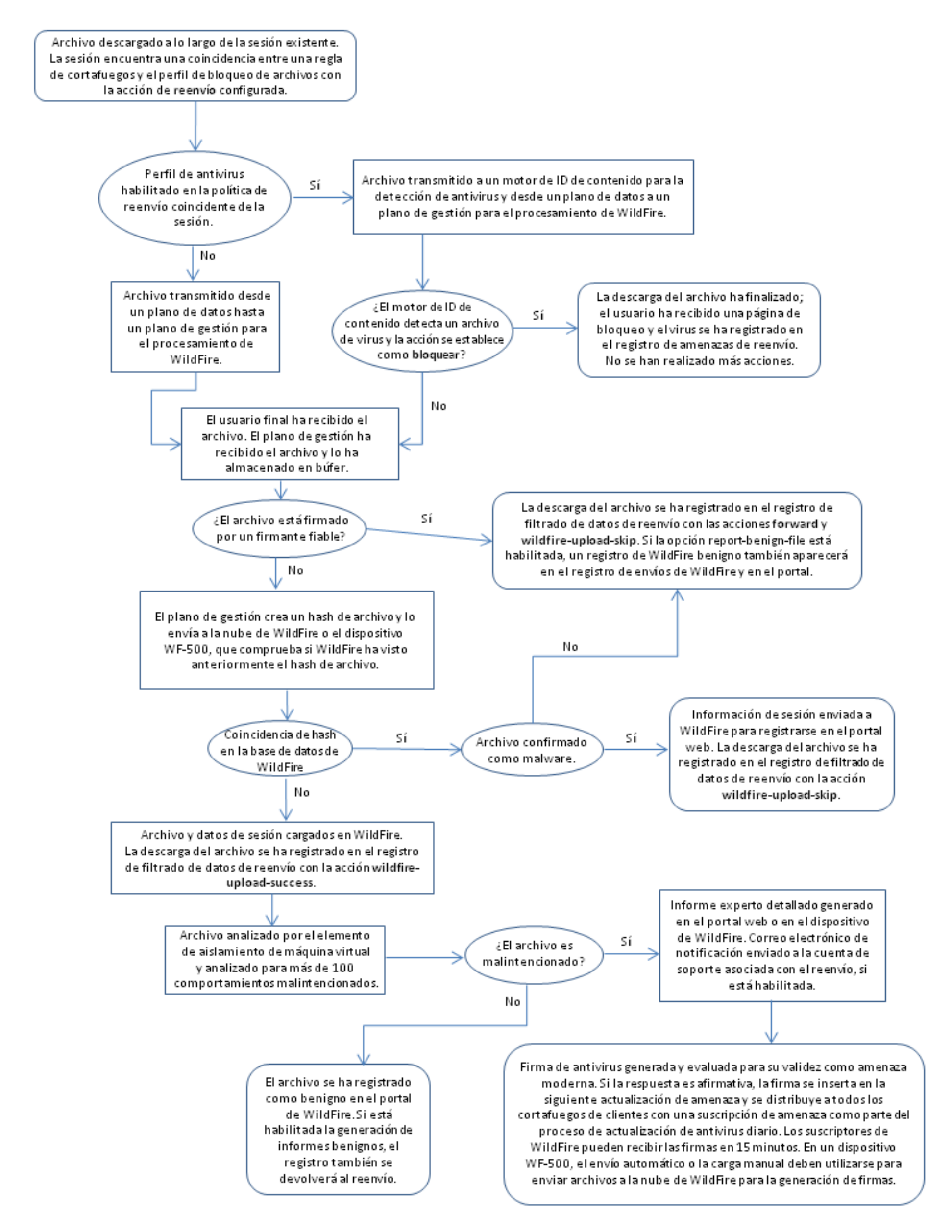
En cuanto el cortafuegos se actualiza con la nueva firma, los archivos que contienen ese malware o una variante de este se eliminarán automáticamente. La información recopilada por WildFire durante el análisis del malware también se usa para fortalecer otras funciones de Threat Prevention, como las categorías de URL de malware PAN-DB, las firmas DNS y las firmas antispyware y antivirus. Palo Alto Networks también desarrolla firmas para el tráfico de comandos y control, lo que permite la interrupción inmediata de la comunicación de cualquier tipo de malware en la red. Si desea más información sobre las ventajas de tener una suscripción de WildFire, consulte ¿Cuáles son las ventajas de la suscripción de WildFire?.

Los siguientes diagramas ilustran el flujo de trabajo de WildFire. La ilustración Flujo de trabajo de decisión de WildFire de alto nivel que aparece a continuación describe el flujo de trabajo de WildFire y la ilustración Flujo de decisión de WildFire detallado proporciona un flujo de trabajo más detallado. Las ilustraciones detalladas muestran el flujo de trabajo de una decisión desde la descarga del archivo inicial por parte de un usuario a través de todo el flujo de trabajo hasta el punto donde se genera una firma si se determina que el archivo es malintencionado.

Flujo de trabajo de decisión de WildFire de alto nivel



Flujo de decisión de WildFire detallado



¿Qué tipos de archivos puede analizar WildFire?

El elemento de aislamiento de WildFire incluye los sistemas operativos Microsoft Windows XP de 32 bits y Windows 7 de 32 bits. Los tipos de archivos que pueden analizarse incluyen los siguientes:

- APK: Paquete de aplicaciones para Android
- PE: Portable Executable, que incluye archivos ejecutables, código objeto, bibliotecas de enlace dinámico (DLL), fuentes FON, etc.
- PDF: Portable Document Format
- Microsoft Office: Incluye documentos (doc, docx), libros de trabajo (xls, xlsx) y PowerPoint (ppt, pptx)
- Java Applet: Tipos de archivo JAR/Class



No se requiere una suscripción para el tipo de archivo PE, pero es obligatoria para el resto de tipos de archivos avanzados (APK, PDF, Microsoft Office y Java Applet). Asimismo, el dispositivo WF-500 WildFire no puede analizar archivos APK.

¿Cómo puedo ver informes en archivos analizados por WildFire?

Por cada archivo que analiza WildFire, se genera un informe detallado de comportamiento unos minutos después del envío del archivo. Estos informes están disponibles en el registro de envíos de WildFire en el cortafuegos, desde el portal de WildFire (https://wildfire.paloaltonetworks.com) o a través de consultas a la API de WildFire. Los informes muestran información detallada de comportamiento sobre el archivo, información sobre el usuario de destino, la aplicación que entregó el archivo y todas las direcciones URL involucradas en la entrega o en la actividad teléfono-casa del archivo. Si desea más información sobre cómo acceder a los informes y a las descripciones de los campos de los informes, consulte Visualización de informes de WildFire.

1 File Information

File Type	PE
File Signer	
SHA-256	bd93a2c673bf90a08bd9ff31f1c023da2d722d3c0ca5bb09462865580e7a41ac
MD5	d11931c7016a350cbf5e0da0352ae514
File Size	739884 bytes
First Seen Timestamp	2013-09-26 23:45:24 UTC
Verdict	Malware
Antivirus Coverage	VirusTotal Information

2 Dynamic Analysis

2.1. VM1 (Windows XP, Adobe Reader 9.4.0, Flash 10, Office 2007)

2.1.1. Behavioral Summary

This sample was found to be **malware** on this virtual machine.

Behavior
Created a file in the Windows folder
Created or modified files
Installed a browser helper object
Spawned new processes
Modified Windows registries
Changed security settings of Internet Explorer
Created an executable file in a user document folder

2.1.2. Network Activity

No network data available.

2.1.3. Host Activity

Process Name - .\4IR4OuzYg.exe

(command: .\4IR4OuzYg.exe)

File Activity

File	Action
C:\Documents and Settings\Administrator\Application Data\Mozilla\Firefox\Profiles\mp6o6ly1.default\extensions\staged\mzav-16@trti-.com\bootstrap.js	Create
C:\Documents and Settings\Administrator\Application Data\Mozilla\Firefox\Profiles\mp6o6ly1.default\extensions\staged\mzav-16@trti-.com\chrome.manifest	Create
C:\Documents and Settings\Administrator\Application Data\Mozilla\Firefox\Profiles\mp6o6ly1.default\extensions\staged\mzav-16@trti-.com\content\bg.js	Create
C:\Documents and Settings\Administrator\Application Data\Mozilla\Firefox\Profiles\mp6o6ly1.default\extensions\staged\mzav-16@trti-.com\install.rdf	Create
C:\Documents and Settings\All Users\Application Data\WXDownlooAed\mqJ4V1qD.dll	Create

¿Qué acciones debo tomar después de que se detecte malware?

Cuando se detecta malware en su red, es importante reaccionar rápido para evitar que se propague a otros sistemas. Para asegurarse de recibir alertas inmediatas de detección de malware en su red, configure sus cortafuegos para que envíen notificaciones de correo electrónico, traps SNMP o Syslog siempre que WildFire devuelva un veredicto de malware sobre un archivo reenviado desde un cortafuegos. Esto le permite ver rápidamente el informe del análisis de WildFire e identificar qué usuario descargó el malware, determinar si el usuario ejecutó el archivo infectado y evaluar si el malware ha intentado propagarse a otros hosts de la red. Si determina que el usuario ejecutó el archivo, puede desconectar rápidamente el equipo de la red para impedir que el malware se propague y seguir los procesos de respuesta a incidentes y reparación según sea necesario. Para obtener más información sobre los informes de WildFire y ver un ejemplo de WildFire en acción, consulte Elaboración de informes de WildFire.

¿Qué implementaciones están disponibles?

El cortafuegos de próxima generación de Palo Alto Networks admite las siguientes implementaciones de WildFire:

- **Nube de WildFire de Palo Alto Networks**: En esta implementación, el cortafuegos reenvía los archivos al entorno de WildFire alojado, que pertenece a Palo Alto Networks y está mantenido por este. Cuando WildFire detecta un nuevo malware, genera nuevas firmas en la hora próxima a la detección. Los cortafuegos equipados con una suscripción de WildFire pueden recibir las nuevas firmas en los siguientes 30-60 minutos; los cortafuegos con solo una suscripción de Threat Prevention pueden recibir las nuevas firmas en la siguiente actualización de firma del antivirus, en las próximas 24-48 horas.

  Los servidores de nube de WildFire disponibles son `wildfire-public-cloud` para la nube de WildFire alojada en EE. UU. y `wildfire.paloaltonetworks.jp` para la nube de WildFire alojada en Japón. Puede que desee utilizar el servidor japonés si no desea que se envíen archivos benignos a los servidores de nube estadounidenses. Si se determina que un archivo enviado a la nube de Japón es malintencionado, este se reenviará a los servidores de EE. UU., donde se volverá a analizar y se generarán las firmas. Si se encuentra en la región de Japón, puede que también experimente una respuesta más rápida en los envíos de muestras y la generación de informes. También se puede configurar Panorama para la nube de Japón.

- **Dispositivo de WildFire**: En esta implementación, instalará un dispositivo WF-500 WildFire en su red empresarial y configurará sus cortafuegos para que reenvíen los archivos a este dispositivo en lugar de a la nube de WildFire de Palo Alto Networks (opción predeterminada). Esta implementación impide que el cortafuegos tenga que enviar archivos fuera de la red para su análisis. De forma predeterminada, el dispositivo no enviará archivos fuera de su red a menos que habilite de forma explícita la función de envío automático, que reenviará automáticamente cualquier malware que detecte a la nube de WildFire de Palo Alto Networks, donde los archivos se analizan para generar firmas de antivirus. Las firmas de antivirus se distribuirán entonces a todos los cortafuegos de Palo Alto Networks con una suscripción de Threat Prevention o WildFire. Un único dispositivo WildFire puede recibir y analizar archivos de hasta 100 cortafuegos de Palo Alto Networks.

Las principales diferencias entre la nube WildFire de Palo Alto Networks y el dispositivo WildFire son las siguientes:

- El dispositivo WildFire habilita el aislamiento local del malware para que los archivos que no resulten peligrosos nunca salgan de la red del cliente. De forma predeterminada, el dispositivo WildFire no reenvía archivos a la nube de WildFire y, por lo tanto, no se generan firmas para el malware detectado por este. Si desea generar firmas de WildFire para el malware detectado en su red, puede habilitar la función de envío automático en el dispositivo. Con esta opción habilitada, el dispositivo envía cualquier malware que detecte a la nube de WildFire para la generación de la firma correspondiente.
- La API de WildFire, que está disponible con una suscripción a WildFire, únicamente puede utilizarse con la nube pública, no con un dispositivo WF-500 privado.
- Se puede realizar un envío manual de muestras en la nube pública a través del portal web (wildfire.paloaltonetworks.com). Con el dispositivo WF-500, no hay ningún portal, así que los registros recibidos desde la aplicación contendrán un enlace en el que se podrá hacer clic para enviar manualmente la muestra a la nube pública. A continuación, la muestra se analizará y se generará una firma si se determina que la muestra es malintencionada. Esto resulta de utilidad si el envío automático no está habilitado.

– Varias máquinas virtuales se ejecutan en la nube de WildFire y representarán una variedad de sistemas operativos y aplicaciones que se utilizan al ejecutar archivos de muestra. En el dispositivo WF-500, hay varias máquinas virtuales disponibles, pero solamente se puede seleccionar una para el análisis de archivos. Al seleccionar qué máquina virtual desea utilizar, puede revisar qué hay instalado y seleccionar la máquina virtual que mejor se adapte a su entorno. Para obtener información sobre cómo visualizar y seleccionar la máquina virtual, consulte Realización de la configuración inicial de WF-500.

¿Cuántos archivos puede reenviar el cortafuegos a WildFire?

La siguiente tabla enumera las plataformas del cortafuegos de Palo Alto Network y el número de archivos que cada plataforma puede enviar a la nube de WildFire o un dispositivo WF-500 por minuto. Si se alcanza el límite por minuto, los archivos se ponen en cola.

Plataforma	Máximo de archivos por minuto	Máximo de archivos simultáneos
PA-200	5	2
PA-500	10	2
PA-2020/2050	20	4
PA-4020	20	4
PA-4050/4060/5020/5050	50	10
PA-5060	100	20
PA-7050	100	20

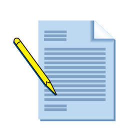
¿Cuáles son las ventajas de la suscripción de WildFire?

WildFire ofrece detección y prevención de malware de día cero mediante una combinación de detección de malware basada en firmas y en aislamiento y bloqueo del malware. No se requiere ninguna suscripción para usar WildFire para el aislamiento de archivos enviados desde cortafuegos de Palo Alto Networks a la nube de WildFire.

Para realizar la detección y el bloqueo de malware conocido detectado por WildFire se requiere una suscripción a Threat Prevention y/o WildFire. La suscripción a Threat Prevention permite al cortafuegos recibir actualizaciones diarias de firma de antivirus, lo que proporciona protección para todas las muestras de malware detectadas por WildFire de forma general para todos los cortafuegos con una suscripción a Threat Prevention. Asimismo, la suscripción de Threat Prevention proporciona acceso a actualizaciones semanales de contenido que incluyen protección frente a vulnerabilidades y firmas antispyware.

Para beneficiarse al completo del servicio WildFire, cada cortafuegos debe tener una suscripción de WildFire, que ofrece las siguientes ventajas:

- **Actualizaciones dinámicas de WildFire**: Nuevas firmas de malware con frecuencias inferiores a una hora. Se pueden configurar en **Dispositivo > Actualizaciones dinámicas**. En la hora siguiente a la detección del nuevo malware, WildFire crea una nueva firma de malware y la distribuye mediante las actualizaciones dinámicas de WildFire, que el cortafuegos puede sondear cada 15, 30 o 60 minutos. El cortafuegos se puede configurar para que realice acciones específicas con respecto a las firmas de malware aparte de las acciones habituales de firma de antivirus del perfil de antivirus. Las firmas de WildFire entregadas en la actualización dinámica incluyen las generadas para el malware detectado en archivos enviados a WildFire por todos los clientes de Palo Alto Networks WildFire, no solo las muestras de archivos que envía el cortafuegos a WildFire.



Una firma de WildFire tarda aproximadamente de 30 a 60 minutos en generarse y en estar disponible para los suscriptores de WildFire después de que el malware se detecte. Los cortafuegos equipados con una suscripción de WildFire pueden sondear la existencia de nuevas firmas de malware cada 15, 30 o 60 minutos. Por ejemplo, si el cortafuegos está definido para sondear actualizaciones de firmas de WildFire cada 30 minutos, puede que no reciba una firma de uno de los archivos enviados hasta el segundo intervalo de sondeo después de que se detecte debido al tiempo que tarda en generarse la firma. Si el cortafuegos solo tiene una suscripción de Threat Prevention, seguirá recibiendo firmas generadas por WildFire después de que las firmas de WildFire entren en las actualizaciones del antivirus, que se producen cada 24-48 horas.

Para los archivos analizados por un dispositivo WF-500 WildFire, solamente se pueden generar firmas para malware detectado en su red si ha habilitado explícitamente la función de envío automático (a menos que el mismo malware haya sido detectado por otro cliente y se haya enviado la misma muestra a la nube pública de WildFire). Si el envío automático está habilitado, el dispositivo reenviará todo el malware detectado a la nube de Palo Alto Networks WildFire, donde se usará para generar una firma de antivirus para detectar y bloquear futuras instancias de malware.

- **Compatibilidad con tipos de archivos avanzados de WildFire**: Además de los archivos PE, una suscripción permite que el cortafuegos también reenvíe los siguientes tipos de archivos avanzados: APK, PDF, Microsoft Office y Java Applet.

- **API de WildFire**: La suscripción a WildFire proporciona acceso a la API de WildFire, lo que permite tener un acceso directo programático al servicio WildFire en la nube de WildFire de Palo Alto Networks. Puede usar la API de WildFire para enviar archivos a la nube de WildFire y recuperar informes de los archivos enviados. La API de WildFire admite hasta 100 envíos de archivos y hasta 1.000 consultas al día. Tenga en cuenta que no puede usar la API de WildFire para enviar archivos al dispositivo WildFire.
- **Dispositivo de WildFire**: Solamente los cortafuegos con una suscripción a WildFire válida pueden reenviar archivos a un dispositivo de WildFire para su análisis. Los cortafuegos que solo tienen una suscripción de Threat Prevention instalada pueden reenviar archivos a la nube de WildFire, pero no a un dispositivo WildFire.

¿Desde dónde puedo acceder a un archivo de muestra de malware para su prueba?

Palo Alto Networks proporciona un archivo de malware de muestra que puede utilizarse para probar una configuración de WildFire en un cortafuegos PAN-OS. Antes de descargar el archivo para comprobar su configuración, asegúrese de que el cortafuegos que se está probando se ha configurado basándose en los procedimientos descritos en Reenvío de archivos a un dispositivo WF-500 WildFire o Envío de archivos a la nube de WildFire.

A continuación se indica información sobre el archivo de prueba:

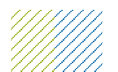
- Cada vez que se hace clic en el enlace de descarga de archivo, se genera y se descarga un archivo único denominado *wildfire-test-pe-file.exe*; además, cada archivo tendrá un valor SHA256 diferente.
- El veredicto del archivo siempre será *malintencionado*.
- Aunque se genera una firma para el archivo, la firma estará deshabilitada y no se distribuirá.

El archivo de prueba puede descargarse haciendo clic en el siguiente enlace: http://wildfire.paloaltonetworks.com/publicapi/test/pe.

Si su cortafuegos tiene habilitado el descifrado, puede acceder a la versión cifrada del sitio sustituyendo HTTP por HTTPS.

Después de descargar el archivo, puede consultar el registro de *filtrado de datos* en el cortafuegos para comprobar si el archivo se ha reenviado y, tras unos cinco minutos, debería ver los resultados en el registro de *envíos de WildFire*. Para obtener más información sobre las verificaciones, consulte los enlaces Verificación de WildFire al reenviar a un dispositivo de WildFire y Verificación de WildFire al reenviar a la nube de WildFire.

Para utilizar la API para recuperar el archivo de prueba de muestra, consulte Uso de la API para recuperar un archivo de prueba de malware de muestra.



Análisis de archivo de WF-500

Esta sección describe el dispositivo WF-500 WildFire y explica cómo configurarlo y gestionarlo para que pueda recibir y analizar archivos. Además, esta sección explica los pasos necesarios para configurar un cortafuegos de Palo Alto Networks para que reenvíe archivos a un dispositivo WildFire, que los analizará.

- ▲ Acerca del dispositivo WF-500 WildFire
- ▲ Configuración del dispositivo WF-500 WildFire
- ▲ Reenvío de archivos a un dispositivo WF-500 WildFire
- ▲ Actualización del software del dispositivo WF-500 WildFire

Acerca del dispositivo WF-500 WildFire

El dispositivo WF-500 WildFire proporciona una nube privada de WildFire in situ, que le permite analizar archivos sospechosos en un entorno aislado sin que sea necesario su envío fuera de la red. Para utilizar un dispositivo WF-500 en lugar de la nube pública de WildFire, configure la nube de WildFire en el cortafuegos para que indique el dispositivo WF-500 en lugar de los servidores de la nube pública de WildFire. El dispositivo WF-500 aísla todos los archivos localmente y los analiza en busca de comportamientos malintencionados usando el mismo motor que el utilizado por el sistema de nube pública de WildFire. En cuestión de minutos, el dispositivo devuelve los resultados del análisis al cortafuegos en el registro de envíos de WildFire.

De forma predeterminada, el dispositivo WF-500 no envía ningún archivo a la nube WildFire de Palo Alto Networks. Sin embargo, se debe enviar el malware a la nube pública de WildFire para poder recibir las firmas del antivirus relacionadas con este software descubierto por el dispositivo. El dispositivo WF-500 tiene una función de envío automático que solamente le permitirá enviar el malware confirmado a la nube pública para la generación de las firmas. Las firmas se distribuyen entonces a todos los clientes que reciben actualizaciones de las firmas de WildFire y del antivirus de Palo Alto Networks. Si no desea habilitar el envío automático, los archivos de muestra se pueden descargar manualmente haciendo clic en el enlace de descarga de archivo del registro de envíos de WildFire del cortafuegos en el área de la pestaña de informe de análisis de WildFire. A continuación, el archivo puede cargarse en el portal de WildFire en https://wildfire.paloaltonetworks.com.

Puede configurar hasta 100 cortafuegos de Palo Alto Networks para que reenvíen archivos a un único dispositivo de WildFire. Cada cortafuegos debe tener una suscripción a WildFire válida para reenviar archivos a un dispositivo de WildFire.

El dispositivo de WildFire tiene dos interfaces:

- **MGT**: Recibe todos los archivos reenviados desde los cortafuegos y devuelve a los cortafuegos los logs que detallan los resultados.
- **Interfaz de la máquina virtual (vm-interface)**: Proporciona acceso a la red para los sistemas de elementos de aislamiento de WildFire para permitir que los archivos de muestra se comuniquen con Internet, lo que permite que WildFire analice mejor el comportamiento de la muestra. Cuando esté configurado, WildFire podrá observar determinados comportamientos malintencionados que no se mostrarían sin un acceso a la red, como la actividad teléfono-casa. Sin embargo, para evitar que el malware acceda a la red desde el elemento de aislamiento, debe asegurarse de configurar esta interfaz en una red aislada con una conexión a Internet. También puede habilitar la opción Tor para ocultar la dirección IP pública de su empresa ante sitios malintencionados a los que pueda acceder la muestra. Para obtener más información sobre la interfaz vm, consulte Configuración de interfaz de la máquina virtual.

Configuración del dispositivo WF-500 WildFire

En esta sección se describen los pasos necesarios para configurar un dispositivo de WildFire en una red y cómo configurar un cortafuegos de Palo Alto Networks para que le reenvíe los archivos para su análisis.

Esta sección contiene los siguientes temas:

▲ Antes de comenzar

▲ Realización de la configuración inicial de WF-500

▲ Verificación de la configuración del dispositivo WF-500 WildFire

▲ Configuración de interfaz de la máquina virtual

▲ Actualización del software del dispositivo WF-500 WildFire

Antes de comenzar

- Monte en un rack el dispositivo WF-500 WildFire y conéctelo. Consulte la *WF-500 WildFire Appliance Hardware Reference Guide (Guía de referencia de hardware de WF-500 WildFire)*.
- Obtenga la información necesaria para configurar la conectividad de la red en el puerto MGT y la interfaz de la máquina virtual desde su administrador de red (dirección IP, máscara de subred, puerta de enlace, nombre de host, servidor DNS). Toda la comunicación entre los cortafuegos y el dispositivo se produce en el puerto MGT, incluidos los envíos de archivo, la distribución de logs de WildFire y la administración de dispositivos. Por lo tanto debe asegurarse de que los cortafuegos tienen conectividad con el puerto MGT del dispositivo. Además, el dispositivo se debe poder conectar al sitio `updates.paloaltonetworks.com` para recuperar las actualizaciones de software del sistema operativo.
- Debe tener preparado un ordenador con un cable de consola o cable Ethernet para conectarse al dispositivo para la configuración inicial.

Realización de la configuración inicial de WF-500

En esta sección se describen los pasos necesarios para instalar un dispositivo WF-500 WildFire en una red y realizar una configuración básica.

Integración del dispositivo WF-500 en una red	
Paso 1 Conecte el ordenador de gestión al dispositivo usando el puerto MGT o el puerto de consola y encienda el dispositivo.	1. Conéctese al puerto de la consola o al puerto MGT. Ambos se encuentran en la parte posterior del dispositivo. • **Puerto de la consola**: Conector serie macho de 9 clavijas. Utilice la siguiente configuración en la aplicación de la consola: 9600-8-N-1. Conecte el cable proporcionado al puerto de serie en el dispositivo de gestión o al conversor USB-serie. • **Puerto MGT**: Puerto RJ-45 Ethernet. De forma predeterminada, la dirección IP del puerto MGT es 192.168.1.1. La interfaz del ordenador de gestión debe estar en la misma subred que el puerto MGT. Por ejemplo, establezca la dirección IP del ordenador de gestión 192.168.1.5. 2. Conecte el dispositivo. **Nota** El dispositivo se activará tan pronto como se encienda la primera fuente de alimentación. Sonará un pitido de advertencia hasta que terminen de conectarse todas las fuentes de alimentación. Si el dispositivo ya está conectado, pero está apagado, utilice el botón de encendido de la parte frontal del dispositivo para encenderlo.
Paso 2 Registre el dispositivo WildFire.	1. Obtenga el número de serie de la etiqueta de número de serie en el dispositivo o ejecute el siguiente comando de la CLI: `admin@WF-500>` **`show system info`** 2. Con un navegador, acceda a https://support.paloaltonetworks.com. 3. Registre el dispositivo de la siguiente forma: Si es el primer dispositivo de Palo Alto Networks que registra y aún no tiene un inicio de sesión, haga clic en **Registrar** en el lado derecho de la página. Para el registro debe proporcionar una dirección de correo electrónico y el número de serie del dispositivo. Cuando se le solicite, establezca un nombre de usuario y una contraseña para acceder a la comunidad de asistencia técnica de Palo Alto Networks. Con las cuentas existentes solo tiene que iniciar sesión y hacer clic en **Mis dispositivos**. Desplácese hasta la sección **Registrar dispositivo**, en la parte inferior de la pantalla, e introduzca el número de serie del dispositivo, su ciudad y su código postal, y haga clic en **Registrar dispositivo**.

Integración del dispositivo WF-500 en una red (Continuación)	
Paso 3 Restablezca la contraseña del administrador.	1. Inicie sesión en el dispositivo con un cliente de SSH o usando el puerto de la consola. Introduzca un nombre de usuario/contraseña de administrador/administrador. 2. Establezca una nueva contraseña ejecutando el comando: `admin@WF-500# set password` 3. Introduzca la contraseña anterior, pulse Intro y, a continuación, introduzca y confirme la nueva contraseña. No hay necesidad de compilar la configuración porque se trata de un comando de operación. 4. Escriba `exit` para cerrar la sesión y, a continuación, vuelva a iniciarla para confirmar que se ha establecido la nueva contraseña.

Paso 4 Establezca la información de IP para la interfaz de gestión y el nombre de host para el dispositivo. Todos los cortafuegos que enviarán archivos al dispositivo WF-500 utilizarán el puerto MGT, por lo que debe asegurase de que esta interfaz es accesible desde estos cortafuegos.
En este ejemplo se utilizan los siguientes valores:
• Dirección IPv4: 10.10.0.5/22
• Máscara de subred: 255.255.252.0
• Puerta de enlace predeterminada: 10.10.0.1
• Nombre de host: wildfire-corp1
• Servidor DNS: 10.0.0.246
	1. Inicie sesión en el dispositivo con un cliente de SSH o usando el puerto de la consola y acceda al modo de configuración.
	`admin@WF-500> configure`
	2. Establezca la información de IP:
	`admin@WF-500# set deviceconfig system ip-address 10.10.0.5 netmask 255.255.252.0 default-gateway 10.10.0.1 dns-setting servers primary 10.0.0.246`
	Nota Puede configurar un servidor DNS secundario sustituyendo “primary” por “secondary” en el comando anterior, excluyendo el resto de parámetros IP. Por ejemplo: `admin@WF-500# set deviceconfig system dns-setting servers secondary 10.0.0.247`
	3. Establezca el nombre del host (*wildfire-corp1* en este ejemplo):
	`admin@WF-500# set deviceconfig system hostname wildfire-corp1`
	4. Compile la configuración para activar la nueva configuración del puerto de gestión externo (MGT):
	`admin@WF-500# commit`
	5. Conecte el puerto de la interfaz de gestión a un conmutador de red.
	6. Vuelva a ubicar el PC de gestión en la red corporativa o en cualquier red necesaria para acceder al dispositivo en la red de gestión.
	7. Desde el ordenador de gestión, conéctese a la nueva dirección IP o nombre de host del puerto de gestión del dispositivo usando un cliente SSH. En este ejemplo, la nueva dirección IP es 10.10.0.5.

Integración del dispositivo WF-500 en una red (Continuación)		

Paso 5	(Opcional) Configure cuentas de usuario adicionales para gestionar el dispositivo WildFire. Se pueden asignar dos funciones: superusuario y superlector. El superusuario es equivalente al administrador, pero el superlector solo tiene acceso de lectura.	En este ejemplo, crearemos una cuenta de superlector para el usuario *bsimpson*:
		1. Introduzca el modo de configuración ejecutando el siguiente comando:
		`admin@WF-500> configure`
		2. Para crear la cuenta de usuario, introduzca el siguiente comando:
		`admin@WF-500# set mgt-config users bsimpson <password>`
		3. Introduzca y confirme la nueva contraseña.
		4. Para asignar la función de superlector, introduzca el siguiente comando y, a continuación, pulse Intro:
		`admin@WF-500# set mgt-config users bsimpson permissions role-based superreader yes`

Paso 6	(Opcional) Configure la autenticación RADIUS para el acceso del administrador. Los pasos siguientes son un resumen de dónde configurar RADIUS en el dispositivo.	1. Cree un perfil de RADIUS mediante las opciones del comando siguiente:
		`admin@WF-500# set shared server-profile radius <profile-name>`
		(Configure el servidor de RADIUS y otros atributos.)
		2. Después de configurar el perfil, cree un perfil de autenticación.
		`admin@WF-500# set shared authentication-profile <profile-name> method radius server-profile <server-profile-name>`
		3. Después de configurar el perfil de autenticación, asigne el perfil a una cuenta de administrador local del modo siguiente:
		`admin@WF-500# set mgt-config users username authentication-profile authentication-profile-name>`

Paso 7	Active el dispositivo con el código de autorización de WildFire que ha recibido de Palo Alto Networks.
	Nota El dispositivo WF-500 funcionará sin un código de autenticación, pero las nuevas actualizaciones de software no pueden instalarse sin un código de autenticación válido.
		1. Vaya al modo de operación para ejecutar los siguientes comandos:
		`admin@WF-500# exit`
		2. Obtenga e instale la licencia de WildFire:
		`admin@WF-500> request license fetch auth-code <auth-code>`
		3. Pulse Intro para obtener e instalar la licencia.
		4. Verifique la licencia:
		`admin@WF-500> request license info`
		Debe aparecer una licencia activa con una fecha posterior a la fecha actual.

Integración del dispositivo WF-500 en una red (Continuación)		

Paso 8	Establezca la fecha/hora actual y la zona horaria.	1. Establezca la fecha y la hora:
		`admin@WF-500> set clock date <YY/MM/DD> time <hh:mm:ss>`
		2. Acceda al modo de configuración:
		`admin@WF-500> configure`
		3. Establezca la zona horaria local:
		`admin@WF-500# set deviceconfig system timezone <timezone>`
		Nota La marca de hora que aparecerá en el informe detallado de WildFire utilizará la zona horaria establecida en el dispositivo. Si hay varias personas viendo estos informes, puede que desee establecer la zona horaria en UTC.

Paso 9	(Opcional) Configure el envío automático para que el dispositivo WildFire envíe archivos que contengan malware a la nube WildFire de Palo Alto Networks. El sistema de nube de WildFire generará firmas, que se distribuyen mediante las actualizaciones de firma de WildFire y del antivirus.
	Nota Esta opción está deshabilitada de manera predeterminada.
		1. Para habilitar el envío automático, ejecute el comando:
		`admin@WF-500# set deviceconfig setting wildfire auto-submit yes`
		2. Para confirmar el ajuste, ejecute el siguiente comando desde el modo de operación:
		`admin@WF-500> show wildfire status`

Paso 10	(Opcional) Habilite el registro de archivos benignos, que es una buena forma de confirmar que los archivos se están reenviando a WildFire sin tener que descargar verdaderos archivos de malware. En este caso, el registro de filtrado de datos contendrá información sobre los resultados de cualquier archivo que haya sido comprobado por WildFire y que se haya determinado que es benigno.
	Nota Esta opción está deshabilitada de manera predeterminada.
		1. Para habilitar el registro de archivos benignos, ejecute el siguiente comando desde el modo de configuración:
		`admin@WF-500# set deviceconfig setting wildfire report-benign-file yes`
		2. Para ver el ajuste en la configuración, ejecute el siguiente comando:
		`admin@WF-500# show deviceconfig setting wildfire`

Integración del dispositivo WF-500 en una red (Continuación)		
Paso 11	Establezca una contraseña para la cuenta de administrador del portal. Esta cuenta se utiliza cuando se accede a los informes de WildFire desde un cortafuegos. El nombre de usuario y la contraseña predeterminados son admin/admin. **Nota** La cuenta del administrador del portal es la única cuenta utilizada para ver informes desde los logs. Solo se puede cambiar la contraseña de esta cuenta; no se pueden crear cuentas adicionales. No es la misma cuenta de administrador utilizada para gestionar el dispositivo.	Para cambiar la contraseña de la cuenta del administrador del portal de WildFire: 1. Introduzca el siguiente comando: `admin@WF-500> set wildfire portal-admin password` 2. Pulse Intro y escriba y confirme la nueva contraseña.

Paso 12	Seleccione la imagen de máquina virtual que mejor se adapte a su entorno. Únicamente puede seleccionar una imagen virtual, que se utilizará para el análisis de archivos. Cada imagen virtual contiene diferentes versiones de sistemas operativos y software, como Windows XP, Windows 7, Adobe Reader y Flash.	Para ver una lista de máquinas virtuales disponibles y determinar cuál representa mejor a su entorno, ejecute el siguiente comando:
		`admin@WF-500> show wildfire vm-images`
		Para ver la imagen de máquina virtual actual, ejecute el siguiente comando y compruebe el campo **Selected VM**:
		`admin@WF-500> show wildfire status`
		Para seleccionar la imagen que se utilizará, entre en el modo de configuración (escriba configure) e introduzca el siguiente comando:
		`admin@WF-500# set deviceconfig setting wildfire active-vm <vm-image-number>`
		Por ejemplo, para utilizar vm-1, ejecute el siguiente comando:
		`admin@WF-500# set deviceconfig setting wildfire active-vm vm-1`

¿Cuál es el siguiente paso?:

- Para verificar la configuración del dispositivo WF-500, consulte Verificación de la configuración del dispositivo WF-500 WildFire.
- Para empezar a enviar archivos desde un cortafuegos, consulte Reenvío de archivos a un dispositivo WF-500 WildFire.
- Para actualizar el software del dispositivo WildFire, consulte Actualización del software del dispositivo WF-500 WildFire.
- Para configurar la interfaz vm que utiliza el dispositivo como parte de su análisis de malware, consulte Configuración de interfaz de la máquina virtual.

Verificación de la configuración del dispositivo WF-500 WildFire

En esta sección se describen los pasos necesarios para verificar la configuración del dispositivo WildFire para garantizar que está listo para recibir archivos desde un cortafuegos de Palo Alto Networks. Para obtener información más detallada sobre los comandos de la CLI a los que se hace referencia en este flujo de trabajo, consulte Referencia de la CLI del software del dispositivo WildFire.

Verificación de la configuración del dispositivo de WildFire	

Paso 1 Compruebe que el dispositivo está registrado y que la licencia se ha activado.	1. Inicie una sesión SSH en la interfaz de gestión del dispositivo.
	2. Desde la CLI, introduzca el siguiente comando:
	`admin@WF-500> request license info`
	3. Compruebe que la licencia es válida y que el valor del campo `Expired:` aparece como `no`.
	Por ejemplo:
	`Feature: Premium`
	`Description: 24x7 phone support; advanced replacement hardware service`
	`serial: 009707000000`
	`Issued: February 11, 2013`
	`Expires: February 11, 2016`
	`Expired?: no`
	4. En aquellos dispositivos habilitados para el envío automático, compruebe que el dispositivo WildFire se puede comunicar con la nube WildFire de Palo Alto Networks introduciendo el siguiente comando:
	`admin@WF-500> test wildfire registration`
	El siguiente resultado indica que el dispositivo está registrado en uno de los servidores de nube WildFire de Palo Alto Networks. Si el envío automático está habilitado, los archivos infectados con malware se enviarán a este servidor.
	`Test wildfire`
	`wildfire registration: successful`
	`download server list:  successful`
	`select the best server:`
	`cs-s1.wildfire.paloaltonetworks.com`
	Nota El dispositivo sólo enviará archivos a la nube de WildFire si el envío automático está habilitado. Para obtener información sobre cómo habilitar el envío automático, consulte las instrucciones de Realización de la configuración inicial de WF-500.

Verificación de la configuración del dispositivo de WildFire (Continuación)		

Paso 2	Compruebe el estado del servidor WildFire en el dispositivo.	1. El siguiente comando muestra el estado de WildFire:
		`admin@WF-500> show wildfire status`
		A continuación aparece un resultado de ejemplo:
		`Connection info:`
		`Wildfire cloud: wildfire-public-cloud`
		`Status: Idle`
		`Auto-Submit: enabled`
		`Select VM: vm-1`
		`VM internet connection: disabled`
		`VM network using Tor: disabled`
		`Best server:`
		`Device registered: yes`
		`Service route IP address: 192.168.2.20`
		`Signature verification: enable`
		`Server selection: enable`
		`Through a proxy: no`
		En este ejemplo, el envío automático está habilitado. El estado `Idle` indica que el dispositivo está listo para recibir archivos. `Device registered` muestra `yes`, lo que significa que el dispositivo está registrado en el sistema de nube de WildFire. El dispositivo también está utilizando vm-1, que es el elemento de aislamiento de la máquina virtual en el que se analizarán las muestras.
		2. Después de configurar sus cortafuegos para que reenvíen archivos al dispositivo según se describe en Reenvío de archivos a un dispositivo WF-500 WildFire, puede verificar el estado de los cortafuegos desde el dispositivo. Para comprobar que el dispositivo está recibiendo archivos desde los cortafuegos y que está enviando archivos a la nube de WildFire para la generación de firmas (si el envío automático está habilitado), introduzca el siguiente comando:
		`admin@WF-500> show wildfire statistics days 7`
		`Last one hour statistics:`
		`Total sessions submitted : 0`
		`Samples submitted : 0`
		`analyzed : 0`
		`pending : 0`
		`malicious : 0`
		`benign : 0`
		`error : 0`
		`Uploaded : 0`
		`Last 7 days statistics:`
		`Total sessions submitted : 66`
		`Samples submitted : 34`
		`analyzed : 34`
		`pending : 0`
		`malicious : 2`
		`benign : 32`
		`error : 0`
		`Uploaded : 0`
		3. Para ver estadísticas más detalladas, introduzca el siguiente comando:
		`admin@WF-500> show wildfire latest [analysis |samples | sessions | uploads]`
		Por ejemplo, para mostrar detalles sobre los resultados del análisis reciente, introduzca el siguiente comando:
		`admin@WF-500> show wildfire latest analysis`

Verificación de la configuración del dispositivo de WildFire (Continuación)		
Paso 3	Compruebe que los cortafuegos configurados para enviar archivos se han registrado correctamente en el dispositivo WildFire.	1. Introduzca el siguiente comando para que muestre una lista de cortafuegos registrados en el dispositivo: `admin@WF-500>` **`show wildfire last-device-registration all`** El resultado debería incluir la siguiente información sobre cada cortafuegos registrado para enviar archivos al dispositivo: número de serie del cortafuegos, fecha de registro, dirección IP, versión de software, modelo de hardware y estado. Si no aparece ningún cortafuegos, puede que haya algún problema de conectividad entre los cortafuegos y el dispositivo. Compruebe la red para confirmar que los cortafuegos y el dispositivo WildFire se pueden comunicar. Utilice las pruebas de ping desde el dispositivo hasta la dirección de la puerta de enlace o a uno de los cortafuegos configurados para enviar al dispositivo Por ejemplo, si uno de los cortafuegos está en la dirección IP 10.0.5.254, las respuestas se mostrarán cuando se ejecute el siguiente comando de la CLI desde el dispositivo: `admin@WF-500>` **`ping host 10.0.5.254`**
Paso 4	Para verificar la configuración de WildFire en los cortafuegos que están reenviando archivos al dispositivo, consulte Verificación de WildFire al reenviar a un dispositivo de WildFire.	

Configuración de interfaz de la máquina virtual

La interfaz de la máquina virtual proporciona conectividad de red externa desde las máquinas virtuales de los elementos de aislamiento en el dispositivo WF-500. En las siguientes secciones se describe la interfaz de la máquina virtual (interfaz vm) y se proporcionan las instrucciones necesarias para configurarla. También puede habilitar la función Tor con vm-interface, lo cual enmascarará el tráfico malintencionado enviado desde WF-500 a través de vm-interface, de modo que los sitios de malware a los que pueda enviarse el tráfico no puedan detectar su dirección IP de cara al público.

Esta sección también describe los pasos necesarios para conectar vm-interface a un puerto especializado en un cortafuegos de Palo Alto Networks para habilitar la conectividad a Internet.

- ¿Qué es la interfaz de la máquina virtual?
- Configuración de la interfaz de la máquina virtual
- Configuración del cortafuegos para controlar el tráfico de la interfaz de la máquina virtual

¿Qué es la interfaz de la máquina virtual?

Cuando esté configurada y habilitada, la interfaz vm (con la etiqueta **1** en la parte posterior del dispositivo) contará con capacidades de detección de malware mejoradas. Esta interfaz permite que un archivo de muestra que se ejecuta en las máquinas virtuales de WildFire se comunique con Internet y permite a WildFire analizar mejor el comportamiento del archivo de muestra para determinar si muestra las características del malware.

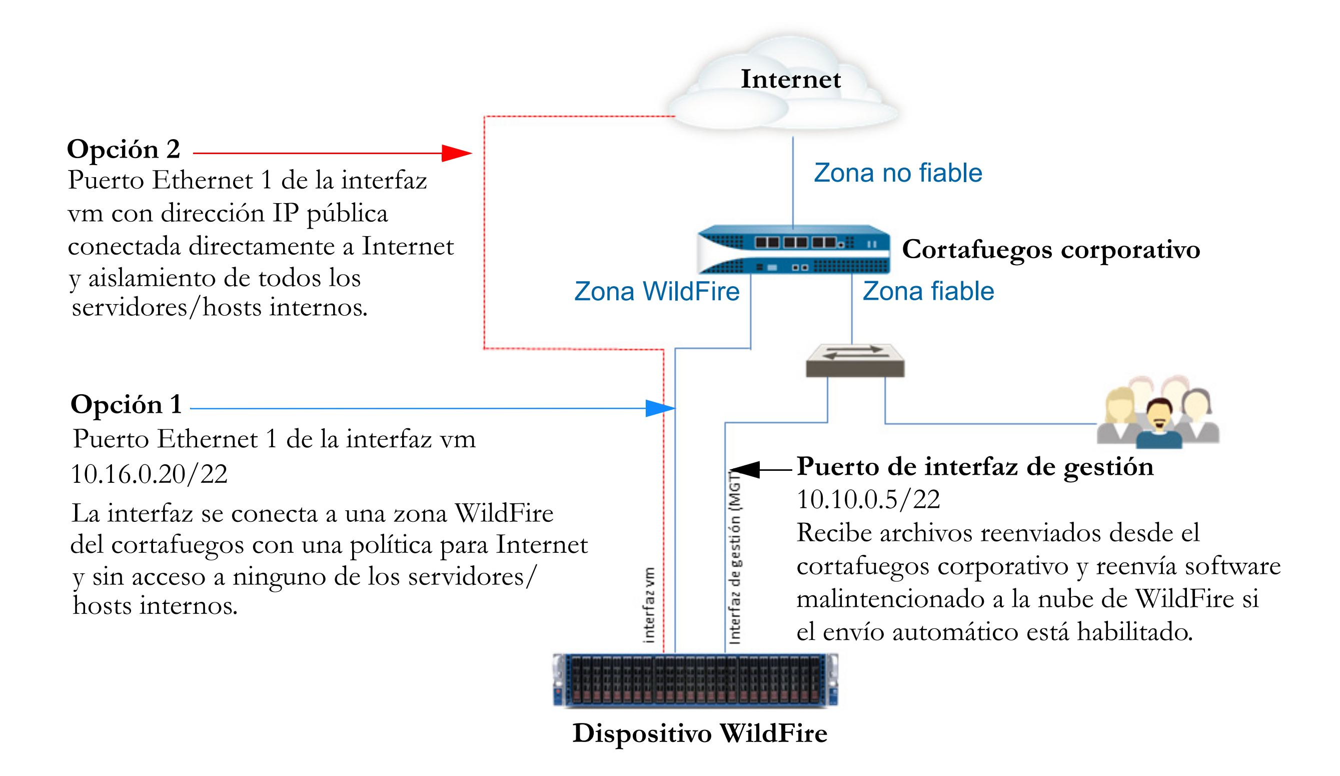


Aunque se recomienda que la interfaz vm esté habilitada, es muy importante que no esté conectada a una red que permita el acceso a cualquiera de los servidores/hosts ya que el malware que se ejecuta en las máquinas virtuales de WildFire podría utilizar esta interfaz para propagarse.

Esta conexión puede ser una línea DSL especializada o un conexión de red que solo permita el acceso directo desde la interfaz a Internet y restrinja cualquier acceso a servidores internos/hosts de cliente.

En la siguiente ilustración se muestran dos opciones para conectar la interfaz vm a la red.

Ejemplo de interfaz de máquina virtual



- **Opción 1 (recomendada)**: Vm-interface se conecta a una interfaz en una zona especializada de un cortafuegos con una política que solamente permite el acceso a Internet. Es importante porque el malware que se ejecuta en las máquinas virtuales de WildFire puede utilizar potencialmente esta interfaz para propagarse. Es la opción recomendada porque los logs del cortafuegos proporcionarán visibilidad en cualquier tráfico generado por la interfaz vm.
- **Opción 2**: Utilice una conexión especializada del proveedor de Internet, como una conexión DSL, para conectar vm-interface a Internet. Asegúrese de que no hay acceso desde esta conexión a servidores/hosts internos. Aunque es una solución simple, el tráfico generado por la interfaz vm no se registrará a no ser que se coloque un cortafuegos o una herramienta de supervisión de tráfico entre el dispositivo WildFire y la conexión DSL.

Configuración de la interfaz de la máquina virtual

Esta sección describe los pasos necesarios para configurar vm-interface en el dispositivo WildFire usando la configuración de la opción 1 detallada en el Ejemplo de interfaz de máquina virtual. Después de configurar la interfaz vm usando esta opción, también debe configurar una interfaz en un cortafuegos de Palo Alto Networks por el que se enrutará el tráfico desde la interfaz vm, según se describe en Configuración del cortafuegos para controlar el tráfico de la interfaz de la máquina virtual.

De forma predeterminada, la interfaz vm está configurada usando los siguientes ajustes:

- Dirección IP: 192.168.2.1
- Máscara de red: 255.255.255.0
- Puerta de enlace predeterminada: 192.168.2.254
- DNS: 192.168.2.254

Si tiene pensado habilitar esta interfaz, configúrela con los ajustes adecuados para la red. Si no tiene pensando utilizar esta interfaz, respete los ajustes predeterminados. La interfaz debe tener valores de red o se producirá un fallo de compilación.

Configuración de la interfaz de la máquina virtual		

Paso 1	Establezca la información de la IP para la interfaz vm en el dispositivo WildFire.
	Se utilizará lo siguiente para este ejemplo:
	• Dirección IPv4: 10.16.0.20/22
	• Máscara de subred: 255.255.252.0
	• Puerta de enlace predeterminada: 10.16.0.1
	• Servidor DNS: 10.0.0.246
	Nota La interfaz vm no puede estar en la misma red que la interfaz de gestión (MGT).
		1. Introduzca el modo de configuración introduciendo el comando de la CLI:
		`admin@WF-500> configure`
		2. Establezca la información de IP para la interfaz vm:
		`admin@WF-500# set deviceconfig system vm-interface ip-address 10.16.0.20 netmask 255.255.252.0 default-gateway 10.16.0.1 dns-server 10.0.0.246`
		Nota Solo se puede asignar un servidor DNS a la interfaz vm. Se recomienda utilizar el servidor NS del ISP o un servicio DNS abierto.

Paso 2	Habilite la interfaz vm.	1. Para habilitar la interfaz vm.
		`admin@WF-500# set deviceconfig setting wildfire vm-network-enable yes`
		2. Confirme la configuración:
		`admin@WF-500# commit`

Paso 3	(Opcional) Habilite la red Tor. Cuando esta opción está habilitada, cualquier tráfico malintencionado que provenga de los sistemas de elementos de aislamiento del WF-500 durante el análisis de muestras se enviará a través de la red Tor. La red Tor enmascarará su dirección IP de cara al público, de modo que los propietarios del sitio web malintencionado no puedan determinar la fuente del tráfico.	Para habilitar la red Tor, ejecute el siguiente comando: 1. `admin@WF-500# set deviceconfig setting wildfire vm-network-use-tor` 2. Confirme la configuración: `admin@WF-500# commit`
Paso 4	Continúe en la siguiente sección para configurar la interfaz del cortafuegos a la que se conectará la interfaz vm.	Consulte Configuración del cortafuegos para controlar el tráfico de la interfaz de la máquina virtual.

Configuración del cortafuegos para controlar el tráfico de la interfaz de la máquina virtual

En el siguiente flujo de trabajo de ejemplo se describe cómo conectar la interfaz vm a un puerto en un cortafuegos de Palo Alto Networks. Antes de conectar la interfaz vm al cortafuegos, este debe tener una zona no fiable conectada a Internet. En este ejemplo, se configura una nueva zona denominada “wf-vm-zone” para conectar la interfaz vm del dispositivo al cortafuegos. La política asociada con la zona wf-vm solo permitirá la comunicación desde la interfaz vm hasta la zona no fiable.

Configuración de la interfaz del cortafuegos para la red de la máquina virtual	
Paso 1 Configure la interfaz en el cortafuegos al que se conectará la interfaz vm y establezca el enrutador virtual. **Nota** La zona wf-vm configurada en este paso solo se debe utilizar para conectar la interfaz vm desde el dispositivo al cortafuegos. No añada ninguna otra interfaz a la zona wf-vm porque el tráfico en el interior de la zona se habilitará de forma predeterminada, lo que permitiría al tráfico de la interfaz vm acceder a una red distinta a Internet.	1. En la interfaz web del cortafuegos, seleccione **Red > Interfaces** y, a continuación, seleccione una interfaz, por ejemplo **Ethernet1/3**. 2. Seleccione **Tipo de interfaz Capa3**. 3. En la pestaña **Configurar**, cuadro desplegable **Zona de seguridad**, seleccione **Nueva zona**. 4. En el campo **Name (Nombre)** del cuadro de diálogo Zona, introduzca **vf-vm-zone** y, a continuación, haga clic en **ACEPTAR**. 5. En el cuadro desplegable **Enrutador virtual**, seleccione **predeterminado**. 6. Para asignar una dirección IP a la interfaz, seleccione la pestaña **IPv4**, haga clic en **Añadir** en la sección IP e introduzca la dirección IP y la máscara de red para asignarlas a la interfaz, por ejemplo, 10.16.0.0/22. 7. Para guardar la configuración de la interfaz, haga clic en **Aceptar**.

Configuración de la interfaz del cortafuegos para la red de la máquina virtual (Continuación)		
Paso 2	Cree una política de seguridad en el cortafuegos para permitir el acceso desde la interfaz vm a Internet y bloquear todo el tráfico entrante. En este ejemplo, el nombre de la política es *Interfaz VM de WildFire*. Como no se creará una política de seguridad desde la zona no fiable a la zona de interfaz wf-vm, todo el tráfico entrante se bloqueará de forma predeterminada.	1. Seleccione **Políticas > Seguridad** y haga clic en **Añadir** 2. En la pestaña **General**, introduzca un **Nombre**, *Interfaz VM de WildFire* en este ejemplo. 3. En la pestaña **Origen**, establezca la **zona de origen** como **wf-vm-interface**. 4. En la pestaña **Destino**, establezca la **zona de destino** como **No fiable**. 5. En las pestañas **Aplicación** y **Categoría de URL/servicio**, deje de forma predeterminada **Cualquiera**. 6. En la pestaña **Acciones**, establezca **Configuración de acción** como **Permitir**. 7. En **Ajuste de log**, seleccione la casilla de verificación **Log al finalizar sesión**. **Nota** Si le preocupa que alguien pueda añadir de forma accidental otras interfaces a wf-vm-zone, clone la política de seguridad de la interfaz VM de WildFire y, a continuación, en la pestaña **Acción** de la regla clonada, seleccione **Denegar**. Asegúrese de que esta nueva política de seguridad aparece bajo la política de seguridad de la interfaz VM de WildFire. Esto hará que la intrazona implícita active la regla que permite sobrescribir las comunicaciones entre interfaces de la misma zona y denegará/bloqueará cualquier comunicación intrazona.
Paso 3	Conecte los cables.	Conecte físicamente la interfaz vm del dispositivo WildFire al puerto que ha configurado en el cortafuegos (Ethernet 1/3 en este ejemplo) usando un cable RJ-45 directo. La interfaz vm aparece con la etiqueta **1** en la parte posterior del dispositivo.
Paso 4	Compruebe que la interfaz vm está transmitiendo y recibiendo tráfico.	1. Desde el modo de operación de la CLI del dispositivo WildFire ejecute el siguiente comando: admin@WF-500> **show interface vm-interface** 2. Aparecerán todos los contadores de la interfaz. Compruebe que los contadores recibidos/transmitidos han aumentado. Ejecute el siguiente comando para generar tráfico ping: admin@WF-500> **ping source vm-interface-ip host <gateway-ip>** Por ejemplo: admin@WF-500> **ping source 10.16.0.20 host 10.16.0.1**

Reenvío de archivos a un dispositivo WF-500 WildFire

En esta sección se describen los pasos necesarios para la configuración de un cortafuegos de Palo Alto Networks para que empiece a reenviar archivos a un dispositivo WF-500 WildFire y se describe cómo verificar la configuración del dispositivo.

Si sus cortafuegos están gestionados por Panorama, simplifique la administración de WildFire usando plantillas de Panorama para introducir la información del servidor WildFire, el tamaño de archivo permitido y los ajustes de información de la sesión en los cortafuegos. Utilice los grupos de dispositivos de Panorama para configurar e introducir los perfiles de bloqueo de los archivos y las reglas de las políticas de seguridad. En cuanto a PAN 6.0, cuando el cortafuegos reenvíe archivos a WildFire, los registros de WildFire devueltos por el servidor WildFire contendrán información sobre el servidor WildFire que analizó el archivo. Esto significa que cuando visualice registros de WildFire desde Panorama, podrá recuperar el informe desde varios sistemas de WildFire (nube de WildFire, dispositivo WF-500 y/o la nube de WildFire de Japón). En versiones anteriores, el ajuste del servidor WildFire en Panorama tenía que coincidir con el ajuste del servidor WildFire configurado en cada cortafuegos gestionado.



Si hay un cortafuegos entre el cortafuegos que está reenviando los archivos a WildFire y la nube de WildFire o el dispositivo WildFire, asegúrese de que el cortafuegos intermedio permite los puertos necesarios.

- Nube de WildFire: Utiliza el puerto 443 para registro y envío de archivos.
- Dispositivo WildFire: Utiliza el puerto 443 para registro y el 10443 para envío de archivos.

Siga estas instrucciones en todos los cortafuegos que reenviarán archivos al dispositivo WildFire:

Configuración del reenvío al dispositivo WF-500 WildFire		
Paso 1	Compruebe que el cortafuegos tiene una suscripción a WildFire y que las actualizaciones dinámicas están programadas y actualizadas. **Nota** Al configurar una programación de actualización de firmas de WildFire, debe introducir un valor distinto de cero en el campo Minutos pasada la hora.	1. Seleccione **Dispositivo > Licencias** y confirme que el cortafuegos tiene instaladas suscripciones a WildFire y Threat Prevention válidas. 2. Seleccione **Dispositivo > Actualizaciones dinámicas** y haga clic en **Comprobar ahora** para asegurarse de que el cortafuegos tiene las actualizaciones más recientes del antivirus, aplicaciones y amenazas y WildFire. 3. Si las actualizaciones no están programadas, hágalo ahora. Asegúrese de escalonar la programación de las actualizaciones porque solo se puede realizar una cada vez. Consulte Recomendaciones para actualizaciones dinámicas para conocer la configuración recomendada.
Paso 2	Defina el servidor WildFire al que reenviará archivos el cortafuegos para su análisis.	1. Seleccione **Dispositivo > Configuración > WildFire**. 2. Haga clic en el icono de edición **Configuración general**. 3. En el campo **Servidor WildFire**, introduzca la dirección IP o FQDN del dispositivo WF-500 WildFire.

Configuración del reenvío al dispositivo WF-500 WildFire (Continuación)	
Paso 3 Configure el perfil de bloqueo del archivo para definir qué aplicaciones y tipos de archivos activarán el reenvío a WildFire. **Nota** Si selecciona **PE** en la columna **Tipos de archivos** del perfil de objetos para seleccionar una categoría de tipos de archivos, no añada también un tipo de archivo individual que forme parte de esa categoría porque estos produciría entradas redundantes en los registros de filtrado de datos. Por ejemplo, si selecciona PE, no es necesario seleccionar exe porque forma parte de la categoría PE. Esto también es aplicable al tipo de archivo zip, ya que los tipos de archivos admitidos que se compriman se envían automáticamente a WildFire. Si desea garantizar que se reenviarán todos los tipos de archivos de Microsoft Office compatibles, se recomienda que seleccione la categoría **msoffice**. Al seleccionar una categoría en lugar de un tipo de archivo individual también se garantiza que, como la compatibilidad con un nuevo tipo de archivo se añade a una categoría específica, automáticamente pasará a formar parte del perfil de bloqueo del archivo. Si selecciona **Cualquiera**, todos los tipos de archivos admitidos se reenviarán a WildFire.	1. Seleccione **Objetos > Perfiles de seguridad > Bloqueo de archivo**. 2. Haga clic en **Añadir** para añadir un nuevo perfil e introduzca un **Nombre** y una **Descripción**. 3. Haga clic en **Añadir** en la ventana **Perfil de bloqueo de archivo** y, a continuación, haga clic en **Añadir** de nuevo. Haga clic en el campo **Nombres** e introduzca un nombre para la regla. 4. Seleccione las **aplicaciones** que coincidirán con este perfil. Por ejemplo, si selecciona **navegación web** como la aplicación, el perfil coincidirá con cualquier tráfico de la aplicación identificado como "navegación web". 5. En el campo **Tipo de archivo**, seleccione los tipos de archivos que activarán la acción de reenvío. Seleccione **Cualquiera** para reenviar todos los tipos de archivos admitidos por WildFire. 6. En el campo **Dirección**, seleccione **cargar**, **descargar** o **ambos**. Si selecciona **ambos** se activará el reenvío siempre que un usuario trate de cargar o descargar un archivo. 7. Defina una **acción** de la siguiente forma (seleccione **Reenviar** para este ejemplo): • **Reenviar**: el cortafuegos reenviará automáticamente cualquier archivo que coincida con este perfil a WildFire para su análisis, además de distribuir el archivo al usuario. • **Continuar y reenviar**: se le indica al usuario que debe hacer clic en **Continuar** antes de que se produzca la descarga y que se reenvíe el archivo a WildFire. Como aquí se necesita de la acción del usuario en un navegador web, solo es compatible con aplicaciones de navegación web. **Nota** Cuando utilice **Continuar y reenviar**, asegúrese de que la interfaz de entrada (la que recibe en primer lugar el tráfico para sus usuarios) tiene un perfil de gestión adjunto que permite páginas de respuesta. Para configurar un perfil de gestión, seleccione **Red > Perfiles de red > Gestión de interfaz** y seleccione la casilla de verificación **Páginas de respuesta**. Instale el perfil de gestión en la pestaña **Avanzado** en la configuración de la interfaz de entrada. 8. Haga clic en **ACEPTAR** para guardar los cambios.
Paso 4 Para reenviar archivos a WildFire desde sitios web usando el cifrado SSL, habilite el reenvío de contenido descifrado. Para obtener información sobre la configuración del descifrado, consulte la *Palo Alto Networks Getting Started Guide (Guía de inicio de Palo Alto Networks)*. **Nota** Solo puede habilitar esta opción un superusuario.	1. Seleccione **Dispositivo > Configuración > ID de contenido**. 2. Haga clic en el icono de edición de las opciones **Filtrado de URL** y habilite **Permitir reenvío de contenido descifrado**. 3. Haga clic en **ACEPTAR** para guardar los cambios. **Nota** Si el cortafuegos tiene múltiples sistemas virtuales, debe habilitar esta opción por VSYS. En esta situación, seleccione **Dispositivo > Sistemas virtuales**, haga clic en el sistema virtual que desea modificar y seleccione la casilla de verificación **Permitir reenvío de contenido descifrado**.

Configuración del reenvío al dispositivo WF-500 WildFire (Continuación)		
Paso 5	Adjunte el perfil de bloqueo de archivos a una política de seguridad.	1. Seleccione **Políticas > Seguridad**. 2. Haga clic en **Añadir** para crear una nueva política para las zonas a las que está aplicando el reenvío de WildFire o seleccione una política de seguridad existente. 3. En la pestaña **Acciones**, seleccione el perfil **Bloqueo de archivo** en el menú desplegable. **Nota** Si esta regla de seguridad no tiene ningún perfil adjunto, seleccione **Perfiles** en el menú **Tipo de perfil** para habilitar la selección de un perfil de bloqueo de archivos.
Paso 6	(Opcional) Modifique el tamaño máximo del archivo que puede cargar el cortafuegos en WildFire.	1. Seleccione **Dispositivo > Configuración > WildFire**. 2. Haga clic en el icono de edición **Configuración general**. 3. Establezca el tamaño máximo que se enviará para cada tipo de archivo.
Paso 7	(Solo PA-7050) Si está configurando un cortafuegos PA-7050, debe configurarse un puerto en uno de los NPC con el tipo de interfaz **Tarjeta de logs**. Esto se debe a las funciones de tráfico/creación de logs del PA-7050 para evitar saturar el puerto MGT. Cuando el puerto de datos está configurado como tipo **Tarjeta de logs**, el reenvío de logs y el reenvío de archivos de WildFire se enviará a través de dicho puerto en vez de utilizar la ruta de servicio predeterminada. Este puerto se utilizará por la tarjeta de logs directamente y actuará como un puerto de reenvío de logs para Syslog, Correo electrónico, SNMP y reenvío de archivos de WildFire. Tras configurar el puerto, el reenvío de archivos de WildFire utilizará este puerto, así como los siguientes tipos de logs: tráfico, coincidencias HIP, amenazas y logs de WildFire. Si el puerto no está configurado, se mostrará un error de compilación y solo se podrá configurar un puerto con el tipo **Tarjeta de logs**. **Nota** El PA-7050 no reenvía logs a Panorama. Panorama solo consultará la tarjeta de logs del PA-7050 para obtener información.	1. Seleccione **Red > Interfaces** y localice un puerto disponible en un NPC. 2. Seleccione el puerto y cambie el **Tipo de interfaz Tarjeta de logs**. 3. En la ficha **Reenvío de tarjetas de logs**, introduzca la información de IP (IPv4 y/o IPv6) para la red que se utilizará para comunicarse con los sistemas que recibirán logs. Por ejemplo: Servidores Syslog y servidores de correo electrónico. Para garantizar la conectividad para el reenvío de archivos de WildFire a la nube de WildFire o un dispositivo WildFire, como el WF-500. 4. Conecte el puerto que acaba de configurar a un conmutador o enrutador. No es necesario realizar ninguna otra configuración. El PA-7050 utilizará este puerto en el momento que quede activado.
Paso 8	(Opcional) Modifique las opciones de la sesión que definen qué información de sesión se debe registrar en los informes de análisis de WildFire.	1. Haga clic en el icono de edición de **Ajustes de información de sesión**. 2. De forma predeterminada, todos los elementos de información de la sesión aparecerán en los informes. Borre las casillas de verificación que correspondan a campos que desee eliminar de los informes de análisis de WildFire. 3. Haga clic en **ACEPTAR** para guardar los cambios.

Configuración del reenvío al dispositivo WF-500 WildFire (Continuación)	
Paso 9 Compile la configuración.	Haga clic en **Compilar** para aplicar los cambios. Durante la evaluación de la política de seguridad, todos los archivos que cumplan los criterios definidos en la política de bloqueo de archivos se reenviarán a WildFire para su análisis. Para obtener información sobre cómo consultar los informes de los archivos que se han analizado, consulte Elaboración de informes de WildFire. Para obtener instrucciones sobre cómo comprobar la configuración, consulte Verificación de WildFire al reenviar a un dispositivo de WildFire.

Recomendaciones para actualizaciones dinámicas

En la siguiente lista se detallan recomendaciones para conseguir actualizaciones dinámicas en un cortafuegos típico que utilice WildFire y que tenga suscripciones a WildFire y prevención de amenazas. Para un flujo de trabajo más dinámico, utilice Panorama para introducir programaciones de actualización dinámicas en los cortafuegos gestionados usando plantillas de Panorama. Así se garantiza la consistencia entre todos los cortafuegos y se simplifica la gestión de la programación de actualizaciones.

Estas orientaciones proporcionan dos opciones de programación: la programación mínima recomendada y una más agresiva. Si elige un enfoque más agresivo, el dispositivo realizará actualizaciones más frecuentemente, algunas de las cuales pueden ser de gran volumen (más de 100 MB para las actualizaciones de antivirus). De igual forma, raramente se podrían producir errores en actualizaciones de firmas. Por lo tanto, considere retrasar la instalación de nuevas actualizaciones hasta que se no hayan publicado un determinado número de horas. Utilice el campo **Umbral (horas)** para especificar cuánto tiempo se debe esperar tras una publicación antes de realizar una actualización de contenido.

- **Antivirus**: se publican nuevas actualizaciones de contenido antivirus diariamente. Para obtener el contenido más reciente, programe estas actualizaciones diariamente como mínimo. Se puede realizar una programación más agresiva cada hora.
- **Aplicaciones y amenazas**: App-ID nuevo, protección de vulnerabilidad y firmas antispyware se publican como actualizaciones de contenido semanales (normalmente los martes). Para obtener el contenido más reciente, programe estas actualizaciones semanalmente como mínimo. Si desea un enfoque más agresivo, realice una programación diaria que garantice que el cortafuegos recibe el contenido más reciente tan pronto como es publicado (incluidas publicaciones ocasionales de contenido urgente fuera de programación).
- **WildFire**: se publican nuevas firmas de antivirus de WildFire cada 30 minutos. Dependiendo de cuándo se descubre el malware en el ciclo de publicación, la cobertura se proporcionará en forma de firma de WildFire 30-60 minutos después de que WildFire lo descubra. Para conseguir las firmas de WildFire más recientes, programe estas actualizaciones cada hora o cada media hora. Para que la programación sea más agresiva, puede programar la búsqueda de actualizaciones del cortafuegos con una frecuencia de 15 minutos.



Al configurar una programación de actualización de firmas de WildFire desde Dispositivo > Actualizaciones dinámicas > WildFire, debe introducir un valor distinto de cero en el campo Minutos pasada la hora. Por ejemplo, si selecciona que la recurrencia se produzca cada 15 minutos, deberá establecer el campo Minutos pasada la hora con un valor distinto de cero, con un intervalo válido de 1-14 minutos. Para una recurrencia de 30 minutos, el intervalo válido es de 1-29 minutos; para cada hora, de 1-59 minutos.

Aunque las actualizaciones de WildFire pueden entrar en conflicto con la actualización de un antivirus o firma de amenazas, la actualización debe ser finalizar con éxito, ya que es mucho más pequeña que la típica actualización de aplicación/antivirus y firma de amenazas. Cada actualización de WildFire suele contener firmas generadas en los últimos 7 días; en ese momento entran a formar parte de la actualización de la firma antivirus cada 24-48 horas.

Verificación de WildFire al reenviar a un dispositivo de WildFire

En esta sección se describen los pasos necesarios para comprobar la configuración de WildFire en el cortafuegos. Para obtener información sobre un archivo de prueba que se pueda utilizar durante el proceso de verificación, consulte ¿Desde dónde puedo acceder a un archivo de muestra de malware para su prueba?.

Comprobación de la configuración de WildFire en el cortafuegos		

Paso 1	Compruebe las suscripciones de WildFire y prevención de amenazas y el registro de WildFire.
	Nota El cortafuegos debe tener una suscripción a WildFire para reenviar archivos a un dispositivo WildFire.
		1. Seleccione **Dispositivo > Licencias** y confirme que se ha instalado una suscripción a WildFire y Threat Prevention válida. Si no hay instaladas licencias válidas, vaya a la sección **Gestión de licencias** y haga clic en **Recuperar claves de licencia del servidor de licencias**.
		2. Para comprobar que el cortafuegos se puede comunicar con un sistema WildFire, de forma que los archivos se puedan reenviar para su análisis, ejecute el siguiente comando de la CLI:
		`admin@PA-200>` **`test wildfire registration`**
		En la siguiente salida, el cortafuegos indica un dispositivo WildFire. Si el cortafuegos indica la nube de WildFire, mostrará el nombre de host de uno de los sistemas WildFire en la nube de WildFire.
		`Test wildfire`
		`wildfire registration: successful`
		`download server list: successful`
		`select the best server: 192.168.2.20:10443`
		Si los problemas con las licencias continúan, póngase en contacto con su distribuidor o con un ingeniero de sistemas de Palo Alto Networks para confirmar todas las licencias y conseguir un nuevo código de autorización si es necesario.

Comprobación de la configuración de WildFire en el cortafuegos (Continuación)		
Paso 2	Confirme que el cortafuegos está enviando archivos al sistema WildFire correcto.	1. Para determinar a dónde está reenviando archivos el cortafuegos (a la nube de WildFire o a un dispositivo de WildFire), seleccione **Dispositivo > Configuración > WildFire**. 2. Haga clic en el botón de edición **Configuración general**. 3. Si el cortafuegos está reenviando archivos a la nube de WildFire, este campo mostrará **wildfire-public-cloud** para la nube de WildFire de EE. UU. o **wildfire.paloaltonetworks.jp** para la nube de WildFire de Japón. Si el cortafuegos reenvía archivos a un dispositivo de WildFire, aparecerán la dirección IP o FQDN del dispositivo de WildFire.
Paso 3	Compruebe los logs.	1. Seleccione **Supervisar > Logs > Filtrado de datos**. 2. Confirme que los archivos se están reenviando a WildFire consultando la columna **Acción**: • **Reenviar**: Indica que el perfil de bloqueo del archivo y la política de seguridad reenviaron el archivo de forma correcta. • **Wildfire-upload-success**: Indica que el archivo se ha enviado a WildFire. Esto significa que el archivo no está firmado por un firmante de archivo fiable y que WildFire no lo ha analizado anteriormente. • **Wildfire-upload-skip**: Indica que el archivo se identificó como apto para enviarse a WildFire por un perfil de bloqueo de archivos o una política de seguridad, pero que no fue necesario que WildFire lo analizase porque ya se había analizado previamente. En este caso, la acción mostrará **reenviar** aparecerá en el registro de filtrado de datos porque era una acción de reenvío válida, pero que no se envió y analizó en WildFire porque el archivo ya se envió a la nube de WildFire desde otra sesión, posiblemente desde otro cortafuegos. 3. Consulte los registros de WildFire seleccionando **Supervisar > Logs > Envíos de WildFire**. Si se enumeran los registros de WildFire, el cortafuegos está reenviando correctamente los archivos a WildFire y WildFire está devolviendo los resultados del análisis de archivos. Para obtener más información sobre los logs relacionados con WildFire, consulte Acerca de los logs de WildFire.
Paso 4	Cree la política de bloqueo de archivos.	1. Seleccione **Objetos > Perfiles de seguridad > Bloqueo de archivo** y haga clic en el perfil de bloqueo de archivo para modificarlo. 2. Confirme que la acción está establecida en **Reenviar** o en **Continuar y reenviar**. Si está establecida en **Continuar y reenviar**, solo se reenviará el tráfico http/https porque es el único tipo de tráfico que permite solicitar al usuario que haga clic para continuar.
Paso 5	Compruebe la política de seguridad.	1. Seleccione **Políticas > Seguridad** y haga clic en la regla de política de seguridad que activa el reenvío de archivos a WildFire. 2. Haga clic en la pestaña **Acciones** y asegúrese que la política de bloqueo de archivos está seleccionada en el menú desplegable **Bloqueo de archivo**.

Comprobación de la configuración de WildFire en el cortafuegos (Continuación)

Paso 6 Compruebe el estado de WildFire.

Compruebe el estado de WildFire:

admin@PA-200> **show wildfire status**

Cuando reenvíe los archivos a la nube de WildFire, el resultado debería tener un aspecto similar al siguiente:

```
Connection info:
  Wildfire cloud:               public cloud
  Status:                       Idle
  Best server:               s1.wildfire.paloaltonetworks.com
  Device registered:            yes
  Valid wildfire license:       yes
  Service route IP address:     192.168.2.1
  Signature verification:       enable
  Server selection:             enable
  Through a proxy:              no

Forwarding info:
  file size limit for pe (MB):                        10
  file size limit for jar (MB):                        1
  file size limit for apk (MB):                        2
  file size limit for pdf (KB):                      500
  file size limit for ms-office (KB):              10000
  file idle time out (second):                        90
  total file forwarded:                                1
  file forwarded in last minute:                       0
  concurrent files:                                    0
```

Nota Si el cortafuegos está reenviando archivos a un dispositivo de WildFire, el campo `Wildfire cloud:` mostrará la dirección IP o FQDN y `Best server:` no mostrará ningún valor.

Compruebe las estadísticas de WildFire:

Utilice el siguiente comando para comprobar las estadísticas y determinar si los valores han aumentado:

admin@PA-200> **show wildfire statistics**

Este es el resultado de un cortafuegos en funcionamiento. Si no aparece ningún valor, el cortafuegos no está reenviando archivos.

```
Packet based counters:
        Total msg rcvd:                              599
        Total bytes rcvd:                         480074
        Total msg read:                              599
        Total bytes read:                         465698
Total files received from DP: 2
Counters for file cancellation:
Counters for file forwarding:
        file type: apk
        file type: pdf
                FWD_CNT_LOCAL_FILE                     1
                FWD_CNT_REMOTE_FILE                    1
        file type: ms-office
        file type: pe
                FWD_CNT_LOCAL_FILE                     1
                FWD_CNT_REMOTE_DUP_CLEAN               1
        file type: jar
        file type: unknown
        file type: pdns
Error counters:
        FWD_ERR_UNKNOWN_QUERY_RESPONSE                4
        FWD_ERR_CONN_FAIL                             8
Reset counters:
        DP receiver reset cnt:                        2
        File cache reset cnt:                         3
        Service connection reset cnt:                 1
        Log cache reset cnt:                          3
        Report cache reset cnt:                       3
Resource meters:
        data_buf_meter                                0%
        msg_buf_meter                                 0%
        ctrl_msg_buf_meter                            0%
File forwarding queues:
        priority: 1,  size: 0
        priority: 2,  size: 0
```

Comprobación de la configuración de WildFire en el cortafuegos (Continuación)		
Paso 7	Compruebe el estado de las actualizaciones dinámicas y las programaciones para asegurarse de que el cortafuegos está recibiendo automáticamente las firmas generadas por WildFire. **Nota** Al configurar una programación de actualización de firmas de WildFire, debe introducir un valor distinto de cero en el campo Minutos pasada la hora.	1. Seleccione **Dispositivo > Actualizaciones dinámicas**. 2. Asegúrese de que el antivirus, las aplicaciones y amenazas y WildFire tienen las actualizaciones más recientes y que se ha establecido la programación para cada elemento. Escalone la programación de las actualizaciones porque solo se puede realizar una cada vez. 3. Haga clic en **Comprobar ahora** en la parte inferior de las ventanas para ver si hay alguna actualización disponible, lo que también confirma que el cortafuegos se puede comunicar con updates.paloaltonetworks.com. Si el cortafuegos no tiene conectividad con el servidor de actualización, descargue las actualizaciones directamente desde Palo Alto Networks. Inicie sesión en https://support.paloaltonetworks.com y en la sección **Dispositivos gestionados**, haga clic en **Actualizaciones dinámicas** para ver las actualizaciones disponibles. Para obtener más información sobre las actualizaciones dinámicas, consulte la sección Gestión de la actualización de contenidos de la *Palo Alto Networks Getting Started Guide (Guía de inicio de Palo Alto Networks)*.
Paso 8	Para comprobar el estado de registro y las estadísticas de cortafuegos que reenvíen archivos a un dispositivo de WildFire, consulte Verificación de la configuración del dispositivo WF-500 WildFire.	

Actualización del software del dispositivo WF-500 WildFire

En esta sección se proporcionan las instrucciones necesarias para actualizar el software del dispositivo WildFire en un dispositivo WF-500 WildFire. Las actualizaciones de software contienen las últimas características y soluciones de problemas para el software. El dispositivo se puede actualizar usando el servidor de actualización de Palo Alto Networks o descargando e instalando las actualizaciones manualmente (consulte Actualización manual del software). Para obtener detalles sobre una versión específica del software, consulte las notas de la versión correspondiente.

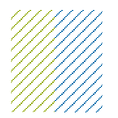
Actualización del software del dispositivo WF-500 WildFire		
Paso 1	Consulte la versión actual del software del dispositivo WildFire en el dispositivo y compruebe si hay una nueva versión disponible.	1. Introduzca el siguiente comando y compruebe el campo `sw-version:` `admin@WF-500>` **`show system info`** 2. Introduzca el siguiente comando para ver las últimas versiones: `admin@WF-500>` **`request system software check`** **Nota** Si el dispositivo no puede ponerse en contacto con el servidor de actualización de Palo Alto Networks, asegúrese de que cuenta con una licencia y de que el DNS está resolviendo correctamente. También puede probar desde el dispositivo haciendo ping al servidor de actualización de Palo Alto Networks para asegurarse de que es posible acceder. Ejecute el siguiente comando de la CLI: `admin@WF-500>` **`ping host updates.paloaltonetworks.com`**
Paso 2	Descargue e instale una nueva versión del software del dispositivo WildFire.	1. Para instalar una nueva versión del software, utilice el siguiente comando: `admin@WF-500>` **`request system software download file <filename>`** Por ejemplo: `admin@WF-500>` **`request system software download file WildFire_m-6.0.0`** 2. Compruebe que el archivo ha terminado de descargarse utilizando el siguiente comando: `admin@WF-500>` **`show jobs pending`** o `admin@WF-500>` **`show jobs all`** 3. Después de se descargue el archivo, instálelo usando el siguiente comando: `admin@WF-500>` **`request system software install file <filename>`** Por ejemplo: `admin@WF-500>` **`request system software install file WildFire_m-6.0.0`** Para instalar por versión: `admin@WF-500>` **`request system software install version <version>`**

Actualización del software del dispositivo WF-500 WildFire (Continuación)	

Paso 3 Después de que se instale la nueva versión, reinicie el dispositivo.	1. Supervise el estado de la actualización usando el siguiente comando:
	`admin@WF-500> show jobs pending`
	2. Después de se actualice el archivo, reinicie el dispositivo usando el siguiente comando:
	`admin@WF-500> request restart system`
	3. Después de reiniciar, verifique que la nueva versión está instalada ejecutando el siguiente comando de la CLI y compruebe el campo `sw-version`:
	`admin@WF-500> show system info`

Actualización manual del software	

Si el dispositivo WildFire no cuenta con conectividad de red a los servidores de actualización de Palo Alto Networks, puede actualizar manualmente el software.	1. Seleccione https://support.paloaltonetworks.com/ y en la sección **Manage Devices (Gestionar dispositivos)**, haga clic en **Software Updates (Actualizaciones de software)**.
	2. Descargue el archivo de imagen del software de WildFire que desea instalar en un ordenador que ejecuta el software del servidor SCP.
	3. Importe el archivo de imagen del software desde el servidor SCP:
	`admin@WF-500> scp import software from <username@ip_address>/<folder_name/imagefile_name>`
	Por ejemplo:
	`admin@WF-500> scp import software from user1@10.0.3.4:/tmp/WildFire_m-6.0.0`
	4. Instale el archivo de imagen:
	`admin@WF-500> request system software install file <image_filename>`
	5. Después de que finalice la actualización, reinicie el dispositivo.
	`admin@WF-500> request restart system`
	6. Después de reiniciar, verifique que la nueva versión está instalada introduciendo el siguiente comando de la CLI y compruebe el campo `sw-version`:
	`admin@WF-500> show system info`



Análisis de archivo de la nube de WildFire

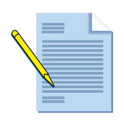
Esta sección describe los pasos necesarios para reenviar archivos desde un cortafuegos de Palo Alto Networks y cargar archivos manualmente utilizando el portal de WildFire o de forma programada utilizando la API de WildFire.

- ▲ Envío de archivos a la nube de WildFire
- ▲ Recomendaciones para actualizaciones dinámicas
- ▲ Verificación de WildFire al reenviar a la nube de WildFire
- ▲ Carga de archivos en el portal de la nube de WildFire
- ▲ Carga de archivos y consulta de WildFire mediante la API de WildFire

Envío de archivos a la nube de WildFire

Para configurar un cortafuegos para el envío automático de archivos a WildFire, configure un perfil de bloqueo de archivo con la acción Reenviar o Continuar y reenviar y, a continuación, adjúntelo a las reglas de seguridad que desea inspeccionar en busca de un malware de día cero. Por ejemplo, podría configurar una política con un perfil de bloqueo de archivo que active el cortafuegos para reenviar un tipo de archivo específico o todos los tipos de archivos admitidos que los usuarios intenten descargar durante una sesión de navegación web. El reenvío de archivos cifrados también es compatible, siempre que el cifrado SSL esté configurado en el cortafuegos y la opción de reenviar archivos cifrados esté activada.

Si sus cortafuegos están gestionados por Panorama, simplifique la administración de WildFire usando plantillas de Panorama para introducir la información del servidor WildFire, el tamaño de archivo permitido y los ajustes de información de la sesión en los cortafuegos. Utilice los grupos de dispositivos de Panorama para configurar e introducir los perfiles de bloqueo de los archivos y las reglas de las políticas de seguridad. En cuanto a PAN 6.0, cuando el cortafuegos reenvíe archivos a WildFire, los registros de WildFire devueltos por el servidor WildFire contendrán información sobre el servidor WildFire que analizó el archivo. Esto significa que cuando visualice registros de WildFire desde Panorama, podrá recuperar el informe desde varios sistemas de WildFire (nube de WildFire, dispositivo WF-500 y/o la nube de WildFire de Japón). En versiones anteriores, el ajuste del servidor WildFire en Panorama tenía que coincidir con el ajuste del servidor WildFire configurado en cada cortafuegos gestionado.



Si hay un cortafuegos entre el cortafuegos que está reenviando los archivos a WildFire y la nube de WildFire o el dispositivo WildFire, asegúrese de que el cortafuegos intermedio permite los puertos necesarios.

- Nube de WildFire: Utiliza el puerto 443 para registro y envío de archivos.
- Dispositivo WildFire: Utiliza el puerto 443 para registro y el 10443 para envío de archivos.

Siga estas instrucciones en todos los cortafuegos que reenviarán archivos a WildFire:

Configuración de un perfil de bloqueo de archivos y posterior adición del mismo a un perfil de seguridad	
Paso 1 Compruebe que el cortafuegos tiene suscripciones a WildFire y prevención de amenazas y que las actualizaciones dinámicas están programadas y actualizadas. **Nota** Tener una suscripción a WildFire ofrece muchas ventajas, como el reenvío de tipos de archivos avanzados, la recepción de firmas de WildFire en menos de 15 minutos, etc. Para obtener más información, consulte ¿Cuáles son las ventajas de la suscripción de WildFire?	1. Seleccione **Dispositivo > Licencias** y confirme que el cortafuegos tiene suscripciones a WildFire y Threat Prevention válidas. 2. Seleccione **Dispositivo > Actualizaciones dinámicas** y haga clic en **Comprobar ahora** para asegurarse de que el cortafuegos tiene las actualizaciones más recientes del antivirus, aplicaciones y amenazas y WildFire. 3. Si las actualizaciones no están programadas, hágalo ahora. Asegúrese de escalonar la programación de las actualizaciones porque solo se puede realizar una cada vez. Consulte Recomendaciones para actualizaciones dinámicas para conocer la configuración recomendada.

Configuración de un perfil de bloqueo de archivos y posterior adición del mismo a un perfil de seguridad		
Paso 2	Configure el perfil de bloqueo del archivo para definir qué aplicaciones y tipos de archivos activarán el reenvío a WildFire. **Nota** Si selecciona **PE** en la columna **Tipos de archivos** del perfil de objetos para seleccionar una categoría de tipos de archivos, no añada también un tipo de archivo individual que forme parte de esa categoría porque estos produciría entradas redundantes en los registros de filtrado de datos. Por ejemplo, si selecciona PE, no es necesario seleccionar exe porque forma parte de la categoría PE. Esto también es aplicable al tipo de archivo zip, ya que los tipos de archivos admitidos que se compriman se envían automáticamente a WildFire. Si desea garantizar que se reenviarán todos los tipos de archivos de Microsoft Office compatibles, se recomienda que seleccione la categoría msoffice. Al seleccionar una categoría en lugar de un tipo de archivo individual también se garantiza que, como la compatibilidad con un nuevo tipo de archivo se añade a una categoría específica, automáticamente pasará a formar parte del perfil de bloqueo del archivo. Si selecciona **Cualquiera**, todos los tipos de archivos admitidos se reenviarán a WildFire.	1. Seleccione **Objetos > Perfiles de seguridad > Bloqueo de archivo**. 2. Haga clic en **Añadir** para añadir un nuevo perfil e introduzca un **Nombre** y una **Descripción**. 3. Haga clic en **Añadir** en la ventana **Perfil de bloqueo de archivo** y, a continuación, haga clic en **Añadir** de nuevo. Haga clic en el campo **Nombres** e introduzca un nombre para la regla. 4. Seleccione las **aplicaciones** que coincidirán con este perfil. Por ejemplo, si selecciona **navegación web** como la aplicación, el perfil coincidirá con cualquier tráfico de la aplicación identificado como "navegación web". 5. En el campo **Tipo de archivo**, seleccione los tipos de archivos que activarán la acción de reenvío. Seleccione **Cualquiera** para reenviar todos los tipos de archivo admitidos por WildFire o seleccione **PE** para que solo reenvíe archivos Portable Executable. 6. En el campo **Dirección**, seleccione **cargar**, **descargar** o **ambos**. La opción **ambos** activará el reenvío siempre que un usuario trate de cargar o descargar un archivo. 7. Defina una **acción** de la siguiente forma: • **Reenviar**: el cortafuegos reenviará automáticamente cualquier archivo que coincida con este perfil a WildFire para su análisis, además de distribuir el archivo al usuario. • **Continuar y reenviar**: se le indica al usuario que debe hacer clic en Continuar antes de que se produzca la descarga y que se reenvíe el archivo a WildFire. Como aquí se necesita de la acción del usuario en un navegador web, solo es compatible con aplicaciones de navegación web. **Nota** Cuando utilice **Continuar y reenviar**, asegúrese de que la interfaz de entrada (la que recibe en primer lugar el tráfico para sus usuarios) tiene un perfil de gestión adjunto que permite páginas de respuesta. Para configurar un perfil de gestión, seleccione **Red > Perfiles de red > Gestión de interfaz** y seleccione la casilla de verificación **Páginas de respuesta**. Instale el perfil de gestión en la pestaña **Avanzado** en la configuración de la interfaz de entrada. 8. Haga clic en **ACEPTAR** para guardar los cambios.

Configuración de un perfil de bloqueo de archivos y posterior adición del mismo a un perfil de seguridad	
Paso 3 Para reenviar archivos con cifrado SSL a WildFire, el descifrado debe estar habilitado en el cortafuegos y debe habilitar el reenvío de contenido descifrado. Para obtener más información sobre la configuración del descifrado, consulte la *Palo Alto Networks Getting Started Guide (Guía de inicio de Palo Alto Networks)*. **Nota** Solo puede habilitar esta opción un superusuario.	1. Seleccione **Dispositivo > Configuración > ID de contenido**. 2. Haga clic en el icono de edición de las opciones **Filtrado de URL** y habilite **Permitir reenvío de contenido descifrado**. 3. Haga clic en **ACEPTAR** para guardar los cambios. **Nota** Si el cortafuegos tiene múltiples sistemas virtuales, debe habilitar esta opción por VSYS. En esta situación, seleccione **Dispositivo > Sistemas virtuales**, haga clic en el sistema virtual que desea modificar y seleccione la casilla de verificación **Permitir reenvío de contenido descifrado**.
Paso 4 Adjunte el perfil de bloqueo de archivos a una política de seguridad.	1. Seleccione **Políticas > Seguridad**. 2. Haga clic en **Añadir** para crear una nueva política para las zonas a las que desea aplicar el reenvío de WildFire o seleccione una política de seguridad existente. 3. En la pestaña **Acciones**, seleccione el perfil **Bloqueo de archivo** en el menú desplegable. **Nota** Si esta regla de seguridad no tiene ningún perfil adjunto, seleccione **Perfiles** en el menú **Tipo de perfil** para habilitar la selección de un perfil de bloqueo de archivos.
Paso 5 (Opcional) Modifique el tamaño máximo del archivo permitido para cargar en WildFire.	1. Seleccione **Dispositivo > Configuración > WildFire**. 2. Haga clic en el icono de edición **Configuración general**. 3. Establezca el tamaño máximo que se enviará para cada tipo de archivo.
Paso 6 (Opcional) Modifique las opciones de la sesión que definen qué información de sesión se debe registrar en los informes de análisis de WildFire.	1. Haga clic en el icono de edición de **Ajustes de información de sesión**. 2. De forma predeterminada, todos los elementos de información de la sesión aparecerán en los informes. Borre las casillas de verificación que correspondan a campos que desee eliminar de los informes de análisis de WildFire. 3. Haga clic en **ACEPTAR** para guardar los cambios.

Configuración de un perfil de bloqueo de archivos y posterior adición del mismo a un perfil de seguridad		
Paso 7	(Solo PA-7050) Si está configurando un cortafuegos PA-7050, debe configurarse un puerto en uno de los NPC con el tipo de interfaz **Tarjeta de logs**. Esto se debe a las funciones de tráfico/creación de logs del PA-7050 para evitar saturar el puerto MGT. Cuando el puerto de datos está configurado como tipo **Tarjeta de logs**, el reenvío de logs y el reenvío de archivos de WildFire se enviará a través de dicho puerto en vez de utilizar la ruta de servicio predeterminada. Este puerto se utilizará por la tarjeta de logs directamente y actuará como un puerto de reenvío de logs para Syslog, Correo electrónico, SNMP y reenvío de archivos de WildFire. Tras configurar el puerto, el reenvío de archivos de WildFire utilizará este puerto, así como los siguientes tipos de logs: tráfico, coincidencias HIP, amenazas y logs de WildFire. Si el puerto no está configurado, se mostrará un error de compilación y solo se podrá configurar un puerto con el tipo **Tarjeta de logs**. **Nota** El PA-7050 no reenvía logs a Panorama. Panorama solo consultará la tarjeta de logs del PA-7050 para obtener información.	1. Seleccione **Red > Interfaces** y localice un puerto disponible en un NPC. 2. Seleccione el puerto y cambie el **Tipo de interfaz Tarjeta de logs**. 3. En la ficha **Reenvío de tarjetas de logs**, introduzca la información de IP (IPv4 y/o IPv6) para la red que se utilizará para comunicarse con los sistemas que recibirán logs. Por ejemplo: Servidores Syslog y servidores de correo electrónico. Para garantizar la conectividad para el reenvío de archivos de WildFire a la nube de WildFire o un dispositivo WildFire, como el WF-500. 4. Conecte el puerto que acaba de configurar a un conmutador o enrutador. No es necesario realizar ninguna otra configuración. El PA-7050 utilizará este puerto en el momento que quede activado.
Paso 8	Compile la configuración.	Haga clic en **Compilar** para aplicar los cambios. Durante la evaluación de la política de seguridad, todos los archivos que cumplan los criterios definidos en la política de bloqueo de archivos se reenviarán a WildFire para su análisis. Para obtener información sobre cómo consultar los informes de los archivos que se han analizado, consulte Elaboración de informes de WildFire. Para obtener instrucciones sobre cómo comprobar la configuración, consulte Verificación de WildFire al reenviar a la nube de WildFire.

Recomendaciones para actualizaciones dinámicas

En la siguiente lista se detallan recomendaciones para conseguir actualizaciones dinámicas en un cortafuegos típico que utilice WildFire y que tenga suscripciones a WildFire y prevención de amenazas. Para un flujo de trabajo más dinámico, utilice Panorama para introducir programaciones de actualización dinámicas en los cortafuegos gestionados usando plantillas de Panorama. Así se garantiza la consistencia entre todos los cortafuegos y se simplifica la gestión de la programación de actualizaciones.

Estas orientaciones proporcionan dos opciones de programación: la programación mínima recomendada y una más agresiva. Si elige un enfoque más agresivo, el dispositivo realizará actualizaciones más frecuentemente, algunas de las cuales pueden ser de gran volumen (más de 100 MB para las actualizaciones de antivirus). De igual forma, raramente se podrían producir errores en actualizaciones de firmas. Por lo tanto, considere retrasar la instalación de nuevas actualizaciones hasta que se no hayan publicado un determinado número de horas. Utilice el campo **Umbral (horas)** para especificar cuánto tiempo se debe esperar tras una publicación antes de realizar una actualización de contenido.

- **Antivirus**: se publican nuevas actualizaciones de contenido antivirus diariamente. Para obtener el contenido más reciente, programe estas actualizaciones diariamente como mínimo. Se puede realizar una programación más agresiva cada hora.
- **Aplicaciones y amenazas**: App-ID nuevo, protección de vulnerabilidad y firmas antispyware se publican como actualizaciones de contenido semanales (normalmente los martes). Para obtener el contenido más reciente, programe estas actualizaciones semanalmente como mínimo. Si desea un enfoque más agresivo, realice una programación diaria que garantice que el cortafuegos recibe el contenido más reciente tan pronto como es publicado (incluidas publicaciones ocasionales de contenido urgente fuera de programación).
- **WildFire**: se publican nuevas firmas de antivirus de WildFire cada 30 minutos. Dependiendo de cuándo se descubre el malware en el ciclo de publicación, la cobertura se proporcionará en forma de firma de WildFire 30-60 minutos después de que WildFire lo descubra. Para conseguir las firmas de WildFire más recientes, programe estas actualizaciones cada hora o cada media hora. Para que la programación sea más agresiva, puede programar la búsqueda de actualizaciones del cortafuegos con una frecuencia de 15 minutos.

Verificación de WildFire al reenviar a la nube de WildFire

En esta sección se describen los pasos necesarios para comprobar la configuración de WildFire en el cortafuegos. Para obtener información sobre un archivo de prueba que se pueda utilizar durante el proceso de verificación, consulte ¿Desde dónde puedo acceder a un archivo de muestra de malware para su prueba?.

<table>
<tr><th colspan="3">Comprobación de la configuración de WildFire en el cortafuegos</th></tr>
<tr><td>Paso 1</td><td>Compruebe las suscripciones a WildFire y prevención de amenazas y el registro de WildFire.</td><td>1. Seleccione Dispositivo > Licencias y confirme que se ha instalado una suscripción a WildFire y Threat Prevention válida. Si no hay instaladas licencias válidas, vaya a la sección Gestión de licencias y haga clic en Recuperar claves de licencia del servidor de licencias.
2. Para comprobar que el cortafuegos se puede comunicar con un sistema WildFire, de forma que los archivos se puedan reenviar para su análisis, ejecute el siguiente comando de la CLI:
<code>admin@PA-200> test wildfire registration</code>
En la siguiente salida, el cortafuegos indica la nube de WildFire. Si el cortafuegos está indicando un dispositivo WildFire, mostrará la dirección IP o FQDN del dispositivo.<pre>Test wildfire
        wildfire registration: successful
        download server list: successful
        select the best server:
              s1.wildfire.paloaltonetworks.com</pre>3. Si los problemas con las licencias continúan, póngase en contacto con su distribuidor o con un ingeniero de sistemas de Palo Alto Networks para confirmar todas las licencias y conseguir un nuevo código de autorización si es necesario.</td></tr>
<tr><td>Paso 2</td><td>Confirme que el cortafuegos está enviando archivos al sistema WildFire correcto.</td><td>1. Para determinar si el cortafuegos está reenviando archivos (a la nube WildFire de Palo Alto Networks o a un dispositivo de WildFire), seleccione Dispositivo > Configuración > WildFire.
2. Haga clic en el botón de edición Configuración general.
3. Si el cortafuegos está reenviando archivos a la nube de WildFire, este campo debería mostrar wildfire-public-cloud para la nube de WildFire de EE. UU. o wildfire.paloaltonetworks.jp para la nube de WildFire de Japón. Si el cortafuegos reenvía archivos a un dispositivo de WildFire, aparecerán la dirección IP o FQDN del dispositivo de WildFire. En Panorama, el nombre predeterminado de la nube es wildfire-public-cloud.
Nota La mejor forma de devolver el campo Servidor WildFire a la nube predeterminada es borrar el campo y hacer clic en ACEPTAR. A continuación, se aplicará el ajuste wildfire-default-cloud.</td></tr>
</table>

Comprobación de la configuración de WildFire en el cortafuegos (Continuación)	
Paso 3 Compruebe los logs.	1. Seleccione **Supervisar > Logs > Filtrado de datos**. 2. Confirme que los archivos se están reenviando a WildFire consultando la columna **Acción**: • **Reenviar**: Indica que el perfil de bloqueo del archivo y la política de seguridad reenviaron el archivo de forma correcta. • **Wildfire-upload-success**: Indica que el archivo se ha enviado a WildFire. Esto significa que el archivo no está firmado por un firmante de archivo fiable y que WildFire no lo ha analizado anteriormente. • **Wildfire-upload-skip**: Indica que el archivo se identificó como apto para enviarse a WildFire por un perfil de bloqueo de archivos o una política de seguridad, pero que no fue necesario que WildFire lo analizase porque ya se había analizado previamente. En este caso, la acción de **reenviar** aparecerá en el registro de **Filtrado de datos** porque era una acción de reenvío válida, pero que no se envió y analizó en WildFire porque el archivo ya se envió a la nube WildFire desde otra sesión, posiblemente desde otro cortafuegos. 3. Consulte los registros de WildFire (se necesita suscripción) seleccionando **Supervisar > Logs > Envíos de WildFire**. Si se enumeran los registros de WildFire, el cortafuegos está reenviando correctamente los archivos a WildFire y WildFire está devolviendo los resultados del análisis de archivos. **Nota** Para obtener más información sobre los logs relacionados con WildFire, consulte Acerca de los logs de WildFire.
Paso 4 Cree la política de bloqueo de archivos.	1. Seleccione **Objetos > Perfiles de seguridad > Bloqueo de archivo** y haga clic en el perfil de bloqueo de archivo para modificarlo. 2. Confirme que la acción está establecida en **Reenviar** o en **Continuar y reenviar**. Si está establecida en **Continuar y reenviar**, solo se reenviará el tráfico http/https porque es el único tipo de tráfico que permite solicitar al usuario que haga clic para continuar.
Paso 5 Compruebe la política de seguridad.	1. Seleccione **Políticas > Seguridad** y haga clic en la regla de política de seguridad que activa el reenvío de archivos a WildFire. 2. Haga clic en la pestaña **Acciones** y asegúrese que la política de bloqueo de archivos está seleccionada en el menú desplegable **Bloqueo de archivo**.

Comprobación de la configuración de WildFire en el cortafuegos (Continuación)

Paso 6 Compruebe el estado de WildFire.

`admin@PA-200> show wildfire status`

Cuando reenvíe los archivos a la nube de WildFire, el resultado debería tener un aspecto similar al siguiente:

```
Connection info:
  Wildfire cloud:                public cloud
  Status:                        Idle
  Best server:                s1.wildfire.paloaltonetworks.com
  Device registered:             yes
  Valid wildfire license:        yes
  Service route IP address:      192.168.2.1
  Signature verification:        enable
  Server selection:              enable
  Through a proxy:               no

Forwarding info:
  file size limit for pe (MB):                          10
  file size limit for jar (MB):                          1
  file size limit for apk (MB):                          2
  file size limit for pdf (KB):                        500
  file size limit for ms-office (KB):                10000
  file idle time out (second):                          90
  total file forwarded:                                  1
  file forwarded in last minute:                         0
  concurrent files:                                      0
```

Nota Si el cortafuegos está reenviando archivos a un dispositivo de WildFire, el campo `Wildfire cloud:` mostrará la dirección IP o FQDN y `Best server:` no mostrará ningún valor.

Paso 7 Compruebe las estadísticas de WildFire.

Utilice el siguiente comando para comprobar las estadísticas y determinar si los valores han aumentado:

`admin@PA-200> show wildfire statistics`

Este es el resultado de un cortafuegos en funcionamiento. Si no aparece ningún valor, el cortafuegos no está reenviando archivos.

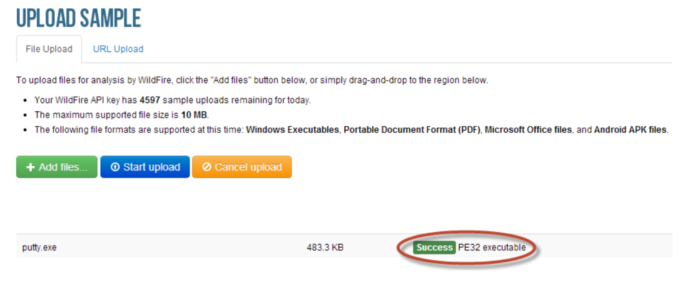
```
Packet based counters:
        Total msg rcvd:                         599
        Total bytes rcvd:                    480074
        Total msg read:                         599
        Total bytes read:                    465698
Total files received from DP: 2
Counters for file cancellation:
Counters for file forwarding:
        file type: apk
        file type: pdf
                FWD_CNT_LOCAL_FILE                1
                FWD_CNT_REMOTE_FILE               1
        file type: ms-office
        file type: pe
                FWD_CNT_LOCAL_FILE                1
                FWD_CNT_REMOTE_DUP_CLEAN          1
        file type: jar
        file type: unknown
        file type: pdns
Error counters:
        FWD_ERR_UNKNOWN_QUERY_RESPONSE           4
        FWD_ERR_CONN_FAIL                        8
Reset counters:
        DP receiver reset cnt:                   2
        File cache reset cnt:                    3
        Service connection reset cnt:            1
        Log cache reset cnt:                     3
        Report cache reset cnt:                  3
Resource meters:
        data_buf_meter                           0%
        msg_buf_meter                            0%
        ctrl_msg_buf_meter                       0%
File forwarding queues:
        priority: 1,  size: 0
        priority: 2,  size: 0
```

Comprobación de la configuración de WildFire en el cortafuegos (Continuación)		
Paso 8	Compruebe el estado de las actualizaciones dinámicas y las programaciones para asegurarse de que el cortafuegos está recibiendo automáticamente las firmas generadas por WildFire.	1. Seleccione **Dispositivo > Actualizaciones dinámicas**. 2. Asegúrese de que el antivirus, las aplicaciones y amenazas y WildFire tienen las actualizaciones más recientes y que se ha establecido la programación para cada elemento. Escalone la programación de las actualizaciones porque solo se puede realizar una cada vez. 3. Haga clic en **Comprobar ahora** en la parte inferior de las ventanas para ver si hay alguna actualización disponible, lo que también confirma que el cortafuegos se puede comunicar con updates.paloaltonetworks.com. Si el cortafuegos no tiene conectividad con el servidor de actualización, descargue las actualizaciones directamente desde Palo Alto Networks. Inicie sesión en https://support.paloaltonetworks.com y en la sección **Dispositivos gestionados**, haga clic en **Actualizaciones dinámicas** para ver las actualizaciones disponibles. Para obtener más información sobre las actualizaciones dinámicas, consulte la sección Gestión de la actualización de contenidos de la *Palo Alto Networks Getting Started Guide (Guía de inicio de Palo Alto Networks)*.

Carga de archivos en el portal de la nube de WildFire

Todos los clientes de Palo Alto Networks con una cuenta de asistencia técnica pueden cargar archivos manualmente en el portal de Palo Alto Networks WildFire para su análisis. El portal de WildFire admite la carga manual de todos los tipos de archivos compatibles.

El siguiente procedimiento describe los pasos necesarios para cargar archivos manualmente:

Carga manual en WildFire		
Paso 1	Cargue un archivo para su análisis en WildFire.	1. Acceda a https://wildfire.paloaltonetworks.com/ o https://wildfire.paloaltonetworks.jp e inicie sesión. 2. Haga clic en el botón **Cargar archivo** en la parte superior derecha de la página y haga clic en **Choose File (Seleccionar archivo)**. 3. Acceda al archivo, resáltelo y, a continuación, haga clic en **Abrir**. El nombre del archivo aparecerá junto a **Choose File (Seleccionar archivo)**. 4. Haga clic en el botón **Upload (Cargar)** para cargar el archivo en WildFire. Si el archivo se carga correctamente, aparecerá un cuadro de diálogo emergente **Uploaded File Information (Información sobre archivo cargado)** parecido al siguiente:  5. Cierre el cuadro de diálogo emergente **Uploaded File Information (Información sobre archivo cargado)**.

Carga manual en WildFire	
Paso 2 Vea los resultados del análisis. WildFire tardará unos 5 minutos en completar el análisis del archivo. **Nota** Como no se asocia la carga manual con un cortafuegos específico, las cargas manuales aparecerán de forma separada de los cortafuegos registrados y no mostrarán información de sesión en los informes.	1. Actualice la página del portal en el navegador. 2. Aparecerá un elemento de línea **Manual** en la lista **Dispositivo** de la página del portal; también aparecerá el resultado del análisis como **malware** o **no peligroso**. Haga clic en la palabra **Manual**. 3. La página del informe mostrará una lista de todos los archivos que se han cargado en su cuenta. Encuentre el archivo cargado y haga clic en el icono de detalles a la izquierda del campo de fecha. El portal muestra un informe completo del análisis de archivo que detalla el comportamiento observado del archivo, incluido el usuario al que estaba destinado, la aplicación que distribuyó el malware y todas las URL relacionadas en la distribución o la actividad teléfono-hogar de la muestra. Si WildFire identifica el archivo como malware, genera una firma que se distribuirá a todos los cortafuegos de Palo Alto Networks configurados para la prevención de amenazas. Los cortafuegos con una suscripción a WildFire pueden descargar estas firmas con una frecuencia inferior a la hora.

Carga de archivos y consulta de WildFire mediante la API de WildFire

La API de WildFire le permite enviar tareas de análisis de archivos de forma programada a la nube de WildFire y pedir al sistema datos de informes mediante una interfaz de API REST sencilla.

Esta sección contiene los siguientes temas:

- Acerca de las suscripciones a WildFire y claves API
- ¿Cómo usar la API de WildFire?
- Métodos de envío de archivos de la API de WildFire
- Consulta de un informe PDF o XML de WildFire
- Uso de la API para recuperar un archivo de prueba de malware de muestra

Acerca de las suscripciones a WildFire y claves API

Se proporciona acceso a la clave API si al menos un cortafuegos de Palo Alto Networks cuenta con una suscripción a Wildfire activa y registrada a nombre de un titular de cuenta de su organización. Puede compartir la misma clave API en la organización. La clave API aparece en la sección **My Account (Mi cuenta)** del portal web de WildFire, junto con estadísticas como cuántas cargas y consultas se han realizado usando la clave. La clave se debe considerar secreta y no debe compartirse fuera de los canales autorizados.

¿Cómo usar la API de WildFire?

La API de WildFire es una API REST que utiliza solicitudes HTTP estándar para enviar y recibir datos. Las llamadas de la API se pueden realizar directamente desde utilidades de la línea de comandos como cURL o usando cualquier secuencia de comandos o marco de aplicaciones que sea compatible con los servicios de la REST.

Los métodos de la API se alojan en https://wildfire.paloaltonetworks.com/ y el protocolo HTTPS (no HTTP) es necesario para proteger su clave API y cualquier otro dato intercambiado con el servicio.

Una clave API de WildFire le permite hasta 100 cargas de muestra por día y hasta 1000 informes por día.

Métodos de envío de archivos de la API de WildFire

Utilice los siguiente métodos para enviar archivos a WildFire:

- Envío de un archivo a la nube de WildFire usando el método de envío de archivo
- Envío de un archivo a WildFire usando el método de envío de URL

Envío de un archivo a la nube de WildFire usando el método de envío de archivo

La API de WildFire se puede utilizar para enviar todos los tipos de archivos compatibles (APK, PE, PDF, Microsoft Office y Java Applet). Al enviar, es necesario el archivo y la clave API para que WildFire abra el archivo en un entorno aislado y lo analice en busca de comportamientos potencialmente malintencionados. El método de envío de archivo devuelve código que un indica un estado satisfactorio o erróneo. Si el resultado es un código 200 OK, significa que el envío ha tenido éxito y que el resultado estará disponible para su consulta en 5 minutos.

La tabla siguiente describe los atributos de la API necesarios para enviar archivos a la nube de WildFire utilizando el método de envío de archivos:

URL	`https://wildfire.paloaltonetworks.com/submit/file`	
Método	`POST`	
Parámetros	`apikey`	Su clave API de WildFire
	`file`	Archivo de muestra que se debe analizar
Resultado	`200 OK`	Indica que la acción se ha realizado correctamente y que se devolverá un informe
	`401 Unauthorized`	Clave API no válida
	`405 Method Not Allowed`	Se ha utilizado un método distinto a POST
	`413 Request Entity Too Large`	Tamaño de archivo de muestra sobre el límite máximo de 10 MB
	`418 Unsupported File Type`	No se admite el tipo de archivo de muestra
	`419 Max Request Reached`	Se ha superado el número máximo de cargas por día
	`500`	Error interno
	`513`	Error al cargar el archivo

Envío de un archivo a WildFire usando el método de envío de URL

Utilice el método de envío de URL para enviar un archivo para su análisis mediante una URL. Este método es idéntico, en cuanto a interfaz y funcionalidad, al método de envío de archivo, aunque un parámetro de URL sustituye al parámetro de archivo. El parámetro de URL debe indicar un tipo de archivo admitido accesible. Si el resultado es un código 200 OK, significa que el envío ha tenido éxito; el resultado suele estar disponible para su consulta en 5 minutos.

La tabla siguiente describe los atributos de la API necesarios para enviar archivos a la nube de WildFire utilizando una URL:

URL	`https://wildfire.paloaltonetworks.com/submit/url`	
Método	`POST`	
Parámetros	`apikey`	Su clave API de WildFire
	`url`	URL del archivo que se debe analizar
Resultado	`200 OK`	Indica que la acción se ha realizado correctamente y que se devolverá un informe

	`401 Unauthorized`	Clave API no válida
	`405 Method Not Allowed`	Se ha utilizado un método distinto a POST
	`413 Request Entity Too Large`	Tamaño de archivo de muestra sobre el límite máximo de 10 MB
	`418 Unsupported File Type`	No se admite el tipo de archivo de muestra
	`419 Max Request Reached`	Se ha superado el número máximo de cargas por día
	`422`	Error de descarga de URL
	`500`	Error interno

Ejemplos de código para el envío de archivos

El siguiente comando cURL muestra cómo enviar un archivo a WildFire utilizando el método de envío de archivos:

```
curl -k  F apikey=yourAPIkey -F  file=@local-file-path
https://wildfire.paloaltonetworks.com/publicapi/submit/file
```

El siguiente ejemplo de código Shell muestra un comando simple para enviar un archivo a la API de WildFire para su análisis. La clave API se proporciona como el primer parámetro y la ruta del archivo es el segundo parámetro:

```
#manual upload sample to WildFire with APIKEY
#Parameter 1: APIKEY
#Parameter 2: location of the file

key=$1
file=$2

/usr/bin/curl -i -k -F apikey=$key -F file=@$file
https://wildfire.paloaltonetworks.com/submit/file
```

El siguiente comando cURL muestra cómo enviar un archivo a WildFire utilizando el método de envío de URL:

```
curl -k  F apikey=yourAPIkey -F  url=URL
https://wildfire.paloaltonetworks.com/publicapi/submit/url
```

Consulta de un informe PDF o XML de WildFire

Utilice el método de obtención de informe para buscar un informe XML o PDF de los resultados del análisis de una muestra concreta. Utilice el hash MD5 o SHA-256 del archivo de muestra como consulta de búsqueda.

La tabla siguiente describe los atributos de la API necesarios para consultar informes:

URL	`https://wildfire.paloaltonetworks.com/publicapi/get/report`	
Método	`POST`	
Parámetros	`hash`	El valor de hash MD5 o SHA-256 de la muestra
	`apikey`	Su clave API de WildFire
	`format`	Formato del informe: PDF o XML

Resultado	`200 OK`	Indica que la acción se ha realizado correctamente y que se devolverá un informe
	`401 Unauthorized`	Clave API no válida
	`404 Not Found`	No se ha encontrado el informe
	`405 Method Not Allowed`	Se ha utilizado un método distinto a POST
	`419`	Se ha excedido la cuota de solicitud de informes
	`420`	Argumentos insuficientes
	`421`	Argumentos no válidos
	`500`	Error interno

Consulta de la API de ejemplo para informe PDF o XML

El siguiente comando cURL muestra una consulta de un informe PDF que usa el hash MD5 de un archivo de muestra:

```
curl -k  -F hash=1234556 -F format=pdf -F apikey=yourAPIkey
https://wildfire.paloaltonetworks.com/publicapi/get/report
```

Nota: Para recuperar la versión XML del informe, sustituya format=pdf por format=xml. Por ejemplo:

```
curl -k  -F hash=1234556 -F format=xml -F apikey=yourAPIkey
https://wildfire.paloaltonetworks.com/publicapi/get/report
```

Uso de la API para recuperar un archivo de prueba de malware de muestra

A continuación se describe la sintaxis de la API para recuperar un archivo de malware de muestra, que se puede utilizar para probar el procesamiento de muestra de WildFire de extremo a extremo.

Para obtener detalles del archivo de muestra, consulte ¿Desde dónde puedo acceder a un archivo de muestra de malware para su prueba?.

Para recuperar el archivo utilizando la API:

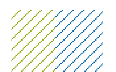
```
API : GET https://wildfire.paloaltonetworks.com/publicapi/test/pe
```

Esto devolverá un archivo de prueba y cada llamada a la API devolverá un archivo similar, pero con un valor SHA256 diferente.

Si hay algún problema al recuperar el archivo, se devolverá el error de servidor interno 500.

Para recuperar el archivo de prueba utilizando cURL:

```
curl -k https://wildfire.paloaltonetworks.com/publicapi/test/pe
```



Elaboración de informes de WildFire

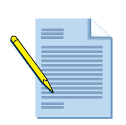
Esta sección describe el sistema de elaboración de informes y registros de WildFire, y en él se le mostrará cómo usar esta información para localizar amenazas e identificar a los usuarios atacados por malware.

- Acerca de los logs de WildFire
- Supervisión de envíos con el portal de WildFire
- Personalización de la configuración del portal de WildFire
- Cuentas de usuario del portal de WildFire
- Visualización de informes de WildFire
- Configuración de alertas para el malware detectado
- WildFire en acción

Acerca de los logs de WildFire

Cada cortafuegos configurado para reenviar archivos a WildFire registrará la acción de reenvío en los registros de filtrado de datos. Después de que WildFire analiza el archivo, si el veredicto es malware, los resultados se devolverán al cortafuegos y aparecerán en los registros de WildFire (se requiere suscripción a WildFire). Para registrar archivos con el veredicto benigno (deshabilitados de manera predeterminada), ejecute el comando de la CLI: `set deviceconfig setting wildfire report-benign-file`.

Puede encontrar el informe de análisis detallado de cada archivo en el log correspondiente de WildFire; para ello, haga clic en el botón **Ver informe de WildFire**. El informe se obtendrá entonces del dispositivo WildFire o de la nube de WildFire. Los informes también pueden visualizarse desde el portal de WildFire en https://wildfire.paloaltonetworks.com.



Si sus cortafuegos reenvían archivos a un dispositivo WildFire para su análisis, los resultados del log solo pueden verse desde el cortafuegos; no hay un acceso directo de portal web al dispositivo.

- **Logs de acción de reenvío**: Los logs de filtrado de datos ubicados en **Supervisar > Logs > Filtrado de datos** mostrarán los archivos que se han bloqueado/reenviado en función del perfil de bloqueo del archivo. Para determinar qué archivos se han reenviado a WildFire, busque los siguientes valores en la columna **Action** (Acción) del log:

Log	Descripción
wildfire-upload-success	El archivo se envió a la nube de WildFire/un dispositivo de WildFire. Esto significa que el archivo no está firmado por un firmante de archivo fiable y que WildFire no lo ha analizado anteriormente.
wildfire-upload-skip	Aparecerá en todos los archivos que se identifiquen como aptos para enviarse a WildFire por un perfil de bloqueo de archivos o una política de seguridad, pero que no fue necesario que WildFire analizase porque ya se habían analizado previamente. En este caso, la acción de **reenviar** aparecerá en el registro de **filtrado de datos** porque era una acción de reenvío válida, pero que no se envió y analizó en WildFire porque el archivo ya se envió a la nube de WildFire o dispositivo de WildFire desde otra sesión, posiblemente desde otro cortafuegos.

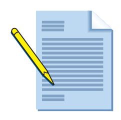
- **Registros de WildFire**: Los resultados del análisis de los archivos analizados por WildFire se devuelven a los registros del cortafuegos una vez se complete el análisis. Estos registros se escriben en el cortafuegos que reenvió el archivo en **Supervisar > Logs > Envíos de WildFire**. Si los logs se reenvían desde el cortafuegos a Panorama, se escriben en el servidor de Panorama, en **Supervisar > Logs > WildFire Submissions (Presentaciones de WildFire)**. La columna **Category (Categoría)** de los logs de WildFire mostrará **benign (Bueno)**, lo que significa que el archivo es seguro, o **malicious (Malintencionado)**, lo que indica que WildFire ha determinado que el archivo contiene código malintencionado. Si se determina que el archivo es malintencionado, el generador de firmas de WildFire generará una firma. Si usa un dispositivo de WildFire, el envío automático debe estar habilitado en el dispositivo para que los archivos infectados con malware se envíen a la nube de WildFire para la generación de la firma.

  De manera predeterminada, los dispositivos con una suscripción a WildFire únicamente recuperarán resultados de análisis desde la nube de WildFire para archivos que se determine que son malware. Para registrar también archivos con el veredicto benigno, ejecute el comando de la CLI: `set deviceconfig setting wildfire report-benign-file`.

Para ver el informe detallado de un archivo analizado por WildFire, localice la entrada del log en el log de WildFire, haga clic en el icono que aparece a la izquierda de la entrada del log para mostrar los detalles y, a continuación, haga clic en el botón **Ver informe de WildFire**. Aparecerá un mensaje de inicio de sesión para acceder al informe y, tras introducir las credenciales correspondientes, el informe se recuperará del sistema WildFire y se mostrará en su explorador. Para obtener información sobre cuentas de portal para acceder a la nube de WildFire, consulte Cuentas de usuario del portal de WildFire. Para obtener información sobre la cuenta de administrador usada para recuperar informes de un dispositivo WildFire, consulte Realización de la configuración inicial de WF-500 y el paso que describe la cuenta portal-admin.

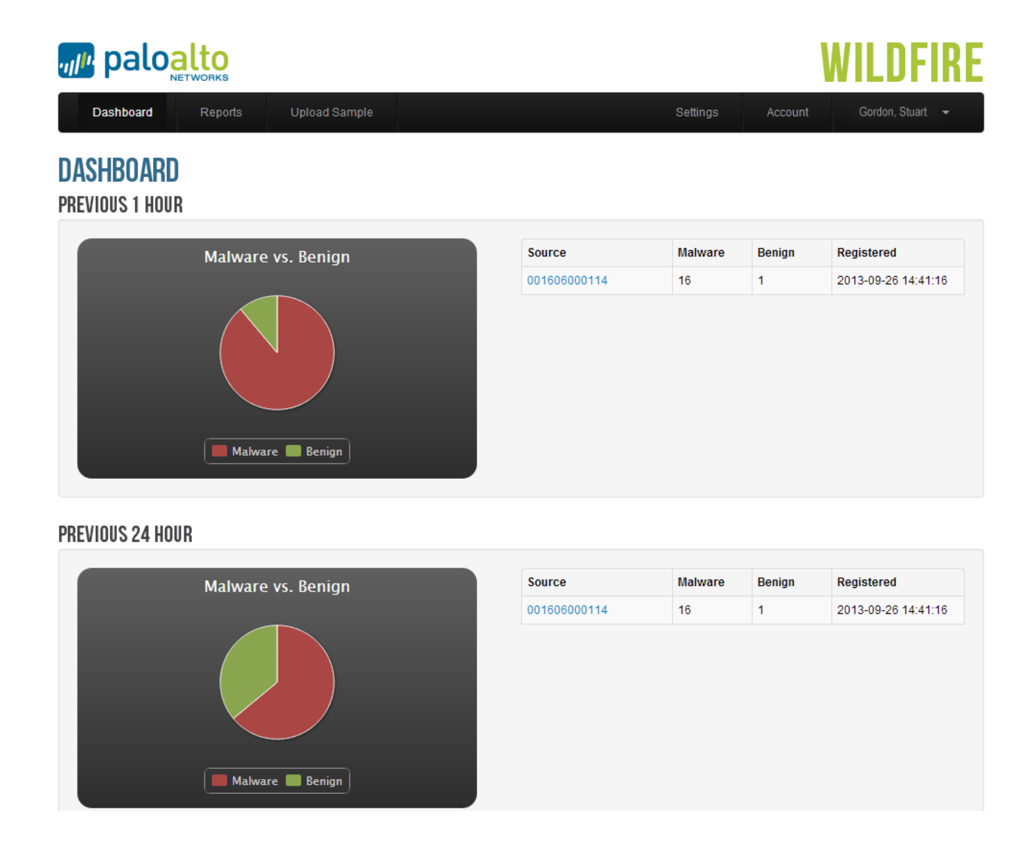
Supervisión de envíos con el portal de WildFire

Vaya a la nube WildFire de Palo Alto Networks, en https://wildfire.paloaltonetworks.com, e inicie sesión usando sus credenciales de asistencia técnica de Palo Alto Networks o su cuenta de WildFire. El portal se abrirá para mostrar el panel, que enumera información de informes de resumen de todos los cortafuegos asociados a la suscripción a WildFire o cuenta de asistencia técnica específica (así como los archivos que se hayan cargado manualmente). Para cada dispositivo, se mostrarán estadísticas del número de archivos de malware detectados, archivos buenos analizados y archivos pendientes en espera para su análisis. También aparecerán la fecha y la hora que registró el cortafuegos la primera vez con el portal para comenzar el reenvío de archivos a WildFire.



Cuando un cortafuegos reenvía archivos a un dispositivo WF-500 WildFire, los informes de WildFire solamente podrán visualizarse desde el registro de envíos de WildFire en el cortafuegos que envió el archivo. No puede ver informes desde el portal de la nube de WildFire, aunque el envío automático esté habilitado en el dispositivo WF-500.

Para obtener información sobre la configuración de cuentas de WildFire adicionales que pueden usarse para revisar información de informes, consulte Cuentas de usuario del portal de WildFire.



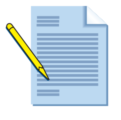
Personalización de la configuración del portal de WildFire

Esta sección describe los ajustes que pueden personalizarse para una cuenta de portal, como la zona horaria y las notificaciones de correo electrónico de cada cortafuegos. También puede eliminar logs de cada cortafuegos que reenvía archivos a la nube de WildFire.

Personalización de la configuración del portal de WildFire		
Paso 1	Configure la zona horaria para la cuenta del portal.	1. Vaya al portal, en https://wildfire.paloaltonetworks.com, e inicie sesión usando sus credenciales de inicio de sesión de asistencia técnica de Palo Alto Networks o su cuenta de usuario de WildFire. 2. Haga clic en el vínculo **Settings** (Configuración), situado en la parte superior derecha de la ventana del portal. 3. Seleccione la zona horaria del menú desplegable y, a continuación, haga clic en **Update Time Zone** (Actualizar zona horaria) para guardar el cambio. **Nota** La marca de hora que aparecerá en el informe detallado de WildFire utilizará la zona horaria establecida en su cuenta del portal.
Paso 2	Elimine los logs de WildFire de cortafuegos específicos. Con esto eliminará todos los logs y las notificaciones del cortafuegos seleccionado.	1. En el menú desplegable **Delete WildFire Logs** (Eliminar logs de WildFire), seleccione el cortafuegos (por número de serie). 2. Haga clic en el botón **Delete Logs** (Eliminar logs). 3. Haga clic en **ACEPTAR** para continuar con la eliminación.
Paso 3	Configure las notificaciones de correo electrónico que se generarán en función de los resultados de los archivos enviados a WildFire. Las notificaciones de correo electrónico se enviarán a la cuenta de correo electrónico registrada en la cuenta de asistencia técnica.	1. Desde la página de configuración del portal, aparecerá una tabla con los encabezados de columna **Device** (Dispositivo), **Malware** (Malware) y **Benign** (Bueno). Marque **Malware** (Malware) y/o **Benign** (Bueno) para cada cortafuegos del que desee recibir notificaciones. Haga clic en **Notificación de actualización** para habilitar las notificaciones para los cortafuegos seleccionados. 2. El primer elemento de la fila mostrará **Manual**. Seleccione **Malware** (Malware) y/o **Benign** (Bueno) para obtener una notificación de los archivos que se han cargado manualmente a la nube de WildFire, o que se han enviado mediante la API de WildFire y haga clic en **Update Notification** para guardar. **Nota** Active las casillas de verificación directamente debajo de los encabezados de columna **Malware** (Malware) y **Benign** (Bueno) para activar todas las casillas de verificación de los dispositivos mostrados.

Cuentas de usuario del portal de WildFire

Las cuentas del portal de WildFire las crea un superusuario (o el propietario registrado de un dispositivo de Palo Alto Networks) para permitir que otros usuarios inicien sesión en el portal web de WildFire y vean datos de WildFire de dispositivos concedidos de forma específica por el superusuario o el propietario registrado. Un superusuario es la persona que ha registrado un cortafuegos de Palo Alto Networks y tiene la principal cuenta de asistencia técnica del dispositivo o los dispositivos. El usuario de WildFire puede ser un usuario del sitio de asistencia técnica existente que pertenezca a cualquier cuenta (incluidas la cuenta secundaria, la principal o cualquier otra cuenta del sistema), o puede ser un usuario que no tenga una cuenta de asistencia técnica de Palo Alto Networks, pero se le ha otorgado acceso solo para el portal de WildFire y un conjunto concreto de cortafuegos.



Cuando un cortafuegos reenvía archivos a un dispositivo WF-500 WildFire, los informes de WildFire solamente podrán visualizarse desde el registro de envíos de WildFire en el cortafuegos que envió el archivo. No puede ver informes desde el portal de la nube de WildFire, aunque el envío automático esté habilitado en el dispositivo WF-500.

Adición de cuentas de usuario de WildFire

Esta sección describe los pasos necesarios para añadir cuentas adicionales de WildFire al portal de WildFire.

Adición de cuentas de usuario de WildFire		
Paso 1	Acceda a la sección para gestionar usuarios y cuentas en el sitio de asistencia técnica y seleccione una cuenta.	1. Inicie sesión en https://support.paloaltonetworks.com/. 2. En **Manage Account** (Gestionar cuenta), haga clic en **Users and Accounts** (Usuarios y cuentas). 3. Seleccione una cuenta o una cuenta secundaria existente.
Paso 2	Añada un usuario de WildFire.	1. Haga clic en el botón **Add WildFire User** (Añadir usuario de WildFire). 2. Introduzca la dirección de correo electrónico del usuario destinatario que desea añadir. **Nota** El usuario puede ser un usuario de sitio de asistencia técnica existente que pertenezca a cualquier cuenta (incluidas la cuenta secundaria, la cuenta principal, Palo Alto Networks o cualquier otra cuenta del sistema), así como cualquier dirección de correo electrónico que no disponga de una cuenta de asistencia técnica. La única restricción es que la dirección de correo electrónico no puede proceder de una cuenta de correo electrónico gratuita basada en web (Gmail, Hotmail, Yahoo, etc.). Si se introduce una cuenta de correo electrónico de un dominio no compatible, se mostrará un mensaje de advertencia.

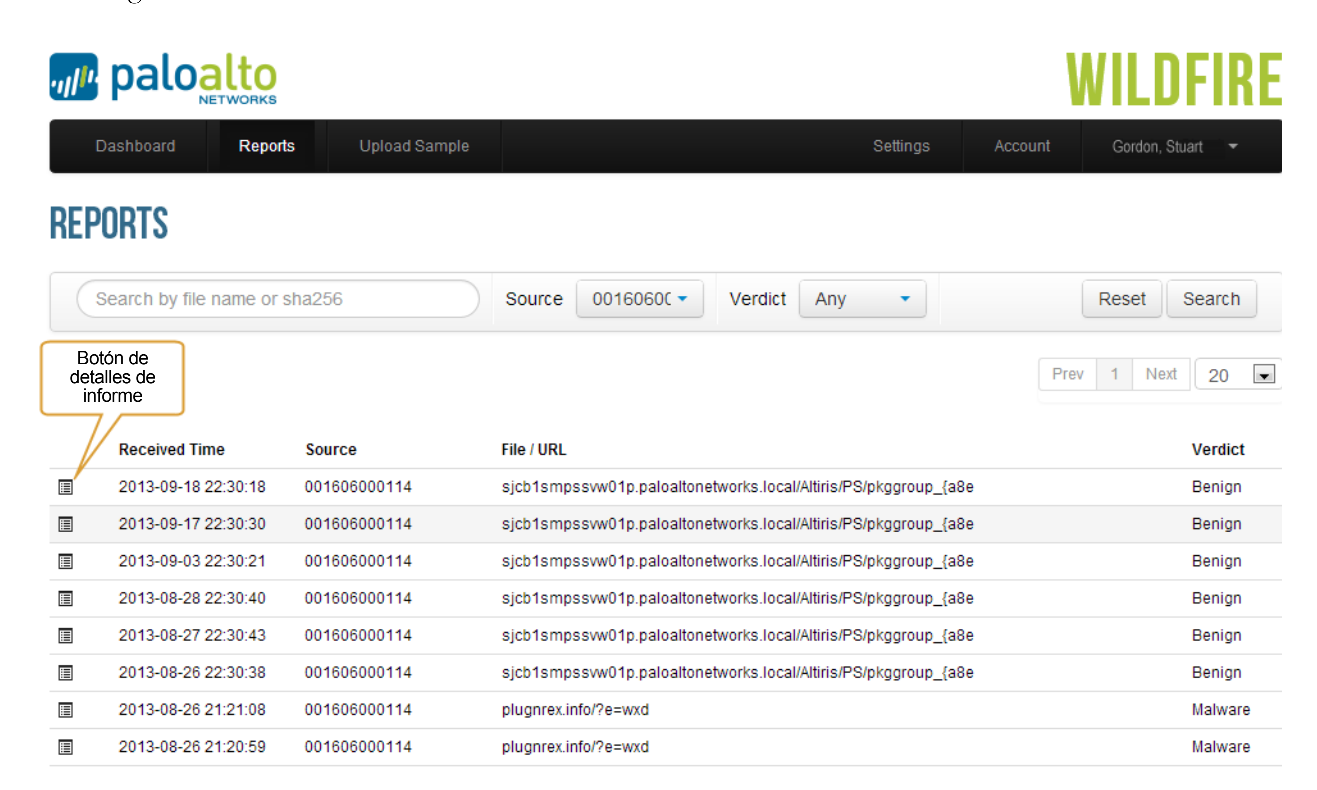
Adición de cuentas de usuario de WildFire (Continuación)		
Paso 3	Asigne cortafuegos a la nueva cuenta de usuario y acceda al portal de WildFire.	1. Seleccione el o los cortafuegos por número de serie a los que desea conceder acceso y cumplimente los detalles de cuenta opcionales. Se enviará un correo electrónico al usuario. Los usuarios con una cuenta de asistencia técnica existente recibirán un correo electrónico con una lista de los cortafuegos de los cuales ahora pueden ver los informes de WildFire. Si el usuario no tiene una cuenta de asistencia técnica, se le enviará un correo electrónico con instrucciones sobre cómo acceder al portal y cómo configurar una nueva contraseña. 2. Los usuarios podrán entonces iniciar sesión en https://wildfire.paloaltonetworks.com y ver informes de WildFire de los cortafuegos a los que se les ha concedido acceso. Además, los usuarios podrán configurar alertas de correo electrónico automáticas para estos dispositivos con el fin de recibir alertas sobre los archivos analizados. También es posible elegir la opción de recibir informes sobre archivos con malware o buenos.

Visualización de informes de WildFire

El método principal para ver informes de WildFire enviados a la nube de WildFire o a un dispositivo de WildFire es acceder al cortafuegos que ha reenviado el archivo a WildFire y, a continuación, seleccionar **Supervisar > Logs > Envíos de WildFire** y seleccionar la pestaña **Informe de análisis de WildFire**. Si el cortafuegos reenvía logs a Panorama, estos pueden verse en Panorama, en la misma área.

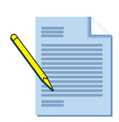
Al enviar archivos al portal de WildFire (mediante el reenvío de cortafuegos, la carga manual o la API de WildFire), es posible acceder a los informes desde el cortafuegos, así como desde el portal de WildFire. Para acceder a los informes desde el portal, inicie sesión en https://wildfire.paloaltonetworks.com y haga clic en el botón **Informes**, en la parte superior de la página del portal de WildFire. Aparecerá una lista que muestre la fecha en la que se ha recibido el archivo, el número de serie del cortafuegos que ha reenviado el archivo (o manual, si el archivo se ha cargado manualmente o mediante la API de WildFire), el nombre de archivo o URL y el veredicto (malware o benigno). La búsqueda también está disponible en la parte superior de la página y puede buscar por nombre de archivo o el valor sha256.

Para ver un informe individual desde el portal, haga clic en el icono **Informes**, situado a la izquierda del nombre del informe. Para guardar el informe detallado, haga clic en el botón **Descargar como PDF** en la esquina superior derecha de la página del informe. A continuación se muestra una lista de archivos de muestra enviados por un cortafuegos:



¿Qué contienen los informes de WildFire?

Los informes de WildFire muestran información detallada de comportamiento sobre el archivo que se ejecutó en el sistema WildFire, así como información sobre el usuario de destino, la aplicación que entregó el archivo y todas las direcciones URL involucradas en la entrega o en la actividad teléfono-casa del archivo. La siguiente tabla describe cada sección que aparece en un informe de análisis de WildFire típico. La organización del informe puede variar en función de la versión del software del dispositivo WildFire instalado en dicho dispositivo, o de si los informes se ven desde la nube de WildFire. El informe contendrá parte o la totalidad de la siguiente información, en función de la información de sesión definida en el cortafuegos que reenvió el archivo, y también en función del comportamiento observado.



Al visualizar un informe de WildFire para un archivo que se ha cargado manualmente al portal de WildFire o mediante la API de WildFire, el informe no mostrará información de sesión, ya que no lo ha reenviado un cortafuegos. Por ejemplo, el informe no mostraría atacante/origen ni víctima/destino.

Encabezado del informe	Descripción
Descargar PDF	• Este botón se encuentra en la esquina superior derecha de cada informe. Haga clic en el botón para descargar una versión PDF del informe de análisis.
Información del archivo	• **Tipo de archivo**: PE, PDF, APK, JAR/Class o MS Office. • **Firmante de archivo**: Entidad que firmó el archivo con el fin de autenticarlo. • **SHA-256**: Muestra la información SHA del archivo. La información SHA es muy similar a una huella digital, que identifica exclusivamente un archivo para garantizar que este no se ha modificado de ninguna forma. • **MD5**: Muestra la información MD5 del archivo. La información MD5 es muy similar a una huella digital, que identifica exclusivamente un archivo para garantizar que este no se ha modificado de ninguna forma. • **Tamaño de archivo**: Tamaño (en bytes) del archivo que se analizó. • **Marca de tiempo de primera visualización**: Si el sistema WildFire ha analizado el archivo anteriormente, esta es la fecha/hora en la que se visualizó por primera vez. • **Verdict (veredicto)**: Muestra el veredicto del análisis: • **Benign (bueno)**: El archivo es seguro y no muestra comportamiento malintencionado. • **Malware (malware)**: WildFire ha identificado el archivo como malware y generará una firma que proteja contra futuras exposiciones. • **Archivo de muestra**: Haga clic en el enlace **Descargar archivo** para descargar el archivo de muestra en su sistema local. • **Cobertura de virus**: Haga clic en este enlace para ver si el archivo se había identificado anteriormente. Esto le llevará al sitio web https://www.virustotal.com/en/, que contiene información sobre varios proveedores de antivirus y le mostrará si estos ofrecen cobertura o no para el archivo infectado. Si el archivo no ha sido detectado nunca antes por ninguno de los proveedores mostrados, aparecerá `file not found` (archivo no encontrado).

Encabezado del informe	Descripción
Información de sesión	Opciones utilizadas para personalizar qué información de sesión incluir en los informes de WildFire para archivos reenviados por un cortafuegos de Palo Alto Networks. La configuración de estas opciones se define en el cortafuegos que envía el archivo de muestra a WildFire y se realiza en la pestaña **Dispositivo > Configuración > WildFire** en la sección Ajustes de información de sesión. Las siguientes opciones están disponibles: • IP de origen • Puerto de origen • IP de destino • Puerto de destino • Sistema virtual (si VSYS múltiple está configurado en el cortafuegos) • Aplicación • Usuario (si el ID de usuarios está configurado en el cortafuegos) • URL • Nombre de archivo
Análisis dinámico	Si un archivo tiene un riesgo bajo y WildFire puede determinar fácilmente que es seguro, solamente se realiza un análisis estático, en lugar de un análisis dinámico. Cuando se realiza un análisis dinámico, esta sección contiene pestañas para cada entorno virtual en el que se ejecutó la muestra al analizar archivos en la nube de WildFire. Por ejemplo, puede que la pestaña Máquina virtual 1 tenga Windows XP, Adobe Reader 9.3.3 y Office 2003 y que Máquina virtual 2 tenga atributos similares, pero con Office 2007. Cuando un archivo se somete a un análisis dinámico completo, se ejecuta en cada máquina virtual y los resultados de cada entorno pueden verse haciendo clic en cualquiera de las pestañas de máquinas virtuales. **Nota** En el dispositivo WF-500 WildFire, el administrador utilizará y seleccionará una máquina virtual basándose en los atributos del entorno virtual que coincidan mejor con el entorno local. Por ejemplo, si la mayoría de los usuarios tienen Windows 7, se seleccionaría dicha máquina virtual.

Encabezado del informe	Descripción
Resumen de comportamientos	Cada pestaña de máquina virtual resume el comportamiento del archivo de muestra en el entorno específico. Algunos ejemplos son si la muestra ha creado o modificado archivos, iniciado un proceso, generado procesos nuevos, modificado el registro o instalado objetos de ayuda del explorador. A continuación se describen los distintos comportamientos que se analizan: • **Actividad de red**: Muestra la actividad de la red realizada por la muestra, como el acceso a otros hosts de la red, consultas DNS y la actividad teléfono-casa. Se proporciona un enlace para descargar la captura de paquete. • **Actividad de host**: Muestra las claves de registro que se han definido, modificado o eliminado. • **Actividad de proceso**: Muestra archivos que han empezado un proceso principal, el nombre del proceso y la acción que ha realizado el proceso. • **Archivo**: Muestra archivos que han empezado un proceso secundario, el nombre del proceso y la acción que ha realizado el proceso. • **Mutex**: Si el archivo de muestra genera otros hilos de ejecución de programa, el nombre de mutex y el proceso principal se registrarán en este campo. • **Línea temporal de actividad**: Proporciona una lista por reproducción de toda la actividad registrada de la muestra. Esto ayudará a comprender la secuencia de eventos que se produjeron durante el análisis. **Nota** La información de línea temporal de actividad solamente está disponible en la exportación a PDF de los informes de WildFire.
Veredicto incorrecto de informe	Haga clic en este enlace para enviar la muestra al equipo de amenazas de Palo Alto Networks si cree que el veredicto es un falso positivo o un falso negativo. El equipo de amenazas realizará más análisis en la muestra para determinar si debería volver a clasificarse. Si se determina que una muestra de malware es segura, la firma del archivo se deshabilitará en una actualización de firma de antivirus futura o, si se determina que un archivo benigno es malintencionado, se generará una nueva firma. Cuando se haya completado la investigación, se enviará un correo electrónico al remitente (si se proporciona una dirección de correo electrónico) sobre el estado de la investigación.

Configuración de alertas para el malware detectado

Esta sección describe los pasos necesarios para configurar un cortafuegos de Palo Alto Networks para enviar una alerta cada vez que WildFire devuelva un log de amenaza al cortafuegos que indica que se ha detectado malware. Las alertas también se pueden configurar desde el portal de WildFire; consulte Supervisión de envíos con el portal de WildFire. Si está utilizando un dispositivo WF-500 y no reenvía archivos a la nube de WildFire utilizando la opción de envío automático, necesitará configurar alertas en el cortafuegos. Este ejemplo describe cómo configurar una alerta de correo electrónico; para configurar Syslog, traps SNMP y/o el reenvío de registros en Panorama, asegúrese de que el cortafuegos esté configurado con los perfiles de servidor necesarios y que esté habilitado el reenvío de registros. Panorama, Syslog o SNMP se pueden seleccionar después junto con el correo electrónico, según se describe en los siguientes pasos:

Para obtener más información sobre alertas y el reenvío de registros, consulte las secciones "Configuración de alertas de correo electrónico", "Definición de servidores Syslog" y "Configuración de los destinos de Trap SNMP" de la *Palo Alto Networks Getting Started Guide (Guía de inicio de Palo Alto Networks)*.

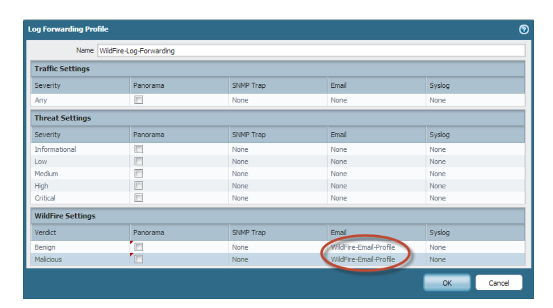
Configuración de alertas de correo electrónico para malware		
Paso 1	Configure un perfil de servidor de correo electrónico si no hay uno ya configurado.	1. Seleccione **Dispositivo > Perfiles de servidor > Correo electrónico**. 2. Haga clic en **Añadir** y, a continuación, introduzca un **Nombre** para el perfil. Por ejemplo, **WildFire-Correoelectronico-Perfil**. 3. (Opcional) Seleccione el sistema virtual al que se aplica este perfil en el menú desplegable **Ubicación**. 4. Haga clic en **Añadir** para añadir una nueva entrada de servidor de correo electrónico e introduzca la información necesaria para conectar con el servidor SMTP y enviar mensajes de correo electrónico (puede añadir hasta cuatro servidores de correo electrónico al perfil): • **Servidor**: Nombre para identificar el servidor de correo electrónico (1-31 caracteres). Este campo es solamente una etiqueta y no tiene que ser el nombre de host de un servidor SMTP existente. • **Mostrar nombre**: El nombre que aparecerá en el campo De del correo electrónico. • **De**: La dirección de correo electrónico desde la que se enviarán las notificaciones de correo electrónico. • **Para**: La dirección de correo electrónico a la que se enviarán las notificaciones de correo electrónico. • **Destinatarios adicionales**: introduzca una dirección de correo electrónico para enviar notificaciones a un segundo destinatario. • **Puerta de enlace**: La dirección IP o el nombre de host de la puerta de enlace SMTP que se usará para enviar los mensajes de correo electrónico. 5. Haga clic en **Aceptar** para guardar el perfil de servidor. 6. Haga clic en **Confirmar** para guardar los cambios en la configuración actual.

<table>
<tr><th colspan="3">Configuración de alertas de correo electrónico para malware (Continuación)</th></tr>
<tr>
<td>Paso 2</td>
<td>Pruebe el perfil del servidor de correo electrónico.</td>
<td>

1. Seleccione **Supervisar > Informes en PDF > Programador de correo electrónico**.
2. Haga clic en **Añadir** y seleccione el nuevo perfil de correo electrónico en el menú desplegable **Perfil de correo electrónico**.
3. Haga clic en el botón **Enviar correo electrónico de prueba** y un correo electrónico de prueba se enviará a los destinatarios definidos en el perfil de correo electrónico.

</td>
</tr>
<tr>
<td>Paso 3</td>
<td>Configure un perfil de reenvío de logs. El perfil de reenvío de logs determina qué tráfico se supervisa y qué gravedad activará una notificación de alerta.</td>
<td>

1. Seleccione **Objetos > Reenvío de logs**.
2. Haga clic en **Añadir** e indique un nombre para el perfil. Por ejemplo, **WildFire-Reenvio-Log**.
3. En la sección **Configuración de WildFire**, seleccione el perfil de correo electrónico de la columna **Correo electrónico** para **Benign** (Bueno) y/o **Malicious** (Malintencionado). El motivo por el que se usa la gravedad media aquí es porque los logs de malware de WildFire tienen una gravedad de tipo **Medio**. Para enviar alertas sobre logs bueno de WildFire, seleccione el tipo de gravedad **Informativo**.
4. Haga clic en **ACEPTAR** para guardar los cambios.



Nota También puede reenviar registros a Panorama y servidores Syslog o enviar traps SNMP. Seleccione la casilla de verificación en la columna de Panorama para habilitarlo o seleccione un perfil para destinos de SNMP o Syslog.

</td>
</tr>
<tr>
<td>Paso 4</td>
<td>Aplique el perfil de reenvío de logs al perfil de seguridad que contiene el perfil de bloqueo de archivos.</td>
<td>

1. Seleccione **Políticas > Seguridad** y haga clic en la política usada para el reenvío de WildFire.
2. En la sección **Ajuste de log** de la pestaña **Acciones**, haga clic en el menú desplegable **Reenvío de logs** y seleccione el nuevo perfil de reenvío de logs. En este ejemplo, el perfil se denomina **WildFire-Reenvio-Log**.
3. Haga clic en **ACEPTAR** para guardar los cambios y, a continuación, haga clic en **Compilar** para confirmar la configuración. Ahora los registros de WildFire se reenviarán a las direcciones de correo electrónico definidas en el perfil de correo electrónico.

</td>
</tr>
</table>

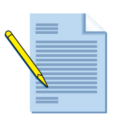
Configuración de alertas de correo electrónico para malware (Continuación)	
Paso 5 (Solo PA-7050) Si está configurando un cortafuegos PA-7050, debe configurarse un puerto en uno de los NPC con el tipo de interfaz **Tarjeta de logs**. Esto se debe a las funciones de tráfico/creación de logs del PA-7050 para evitar saturar el puerto MGT. Cuando el puerto de datos está configurado como tipo **Tarjeta de logs**, el reenvío de logs y el reenvío de archivos de WildFire se enviará a través de dicho puerto en vez de utilizar la ruta de servicio predeterminada. Este puerto se utilizará por la tarjeta de logs directamente y actuará como un puerto de reenvío de logs para Syslog, Correo electrónico, SNMP y reenvío de archivos de WildFire. Tras configurar el puerto, el reenvío de archivos de WildFire utilizará este puerto, así como los siguientes tipos de logs: tráfico, coincidencias HIP, amenazas y logs de WildFire. Si el puerto no está configurado, se mostrará un error de compilación y solo se podrá configurar un puerto con el tipo **Tarjeta de logs**. **Nota** El PA-7050 no reenvía logs a Panorama. Panorama solo consultará la tarjeta de logs del PA-7050 para obtener información.	1. Seleccione **Red > Interfaces** y localice un puerto disponible en un NPC. 2. Seleccione el puerto y cambie el **Tipo de interfaz Tarjeta de logs**. 3. En la ficha **Reenvío de tarjetas de logs**, introduzca la información de IP (IPv4 y/o IPv6) para la red que se utilizará para comunicarse con los sistemas que recibirán logs. Por ejemplo: Servidores Syslog y servidores de correo electrónico. Para garantizar la conectividad para el reenvío de archivos de WildFire a la nube de WildFire o un dispositivo WildFire, como el WF-500. 4. Conecte el puerto que acaba de configurar a un conmutador o enrutador. No es necesario realizar ninguna otra configuración. El PA-7050 utilizará este puerto en el momento que quede activado. 5. **Compile** la configuración.

WildFire en acción

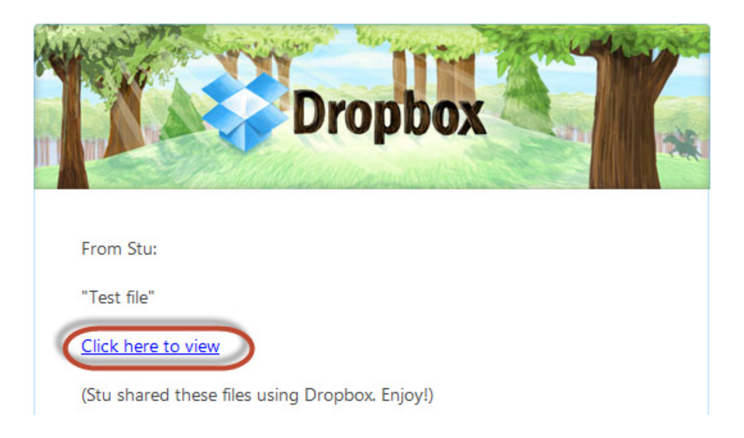
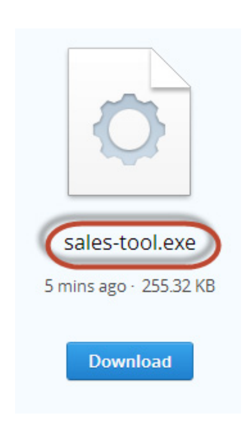
El siguiente caso de ejemplo resume todo el ciclo de vida de WildFire. En este ejemplo, un representante de ventas de Palo Alto Networks descarga una nueva herramienta de ventas de software que un socio de ventas ha cargado en Dropbox. El socio de ventas cargó sin querer una versión infectada del archivo de instalación de la herramienta de ventas, y el representante de ventas descargó después el archivo infectado.

Este ejemplo mostrará cómo el cortafuegos de Palo Alto Networks junto con WildFire puede detectar malware de día cero descargado por sus usuarios incluso cuando el tráfico tiene cifrado SSL. Una vez identificado el malware, se notifica al administrador, se avisa al usuario que descargó el archivo y el cortafuegos descarga automáticamente una nueva firma que proteja frente a futuras exposiciones del malware a través de actualizaciones de antivirus. Aunque algunos sitios web de uso compartido de archivos tienen una función antivirus que comprueba los archivos cuando se cargan, solo pueden proteger contra malware "conocido".

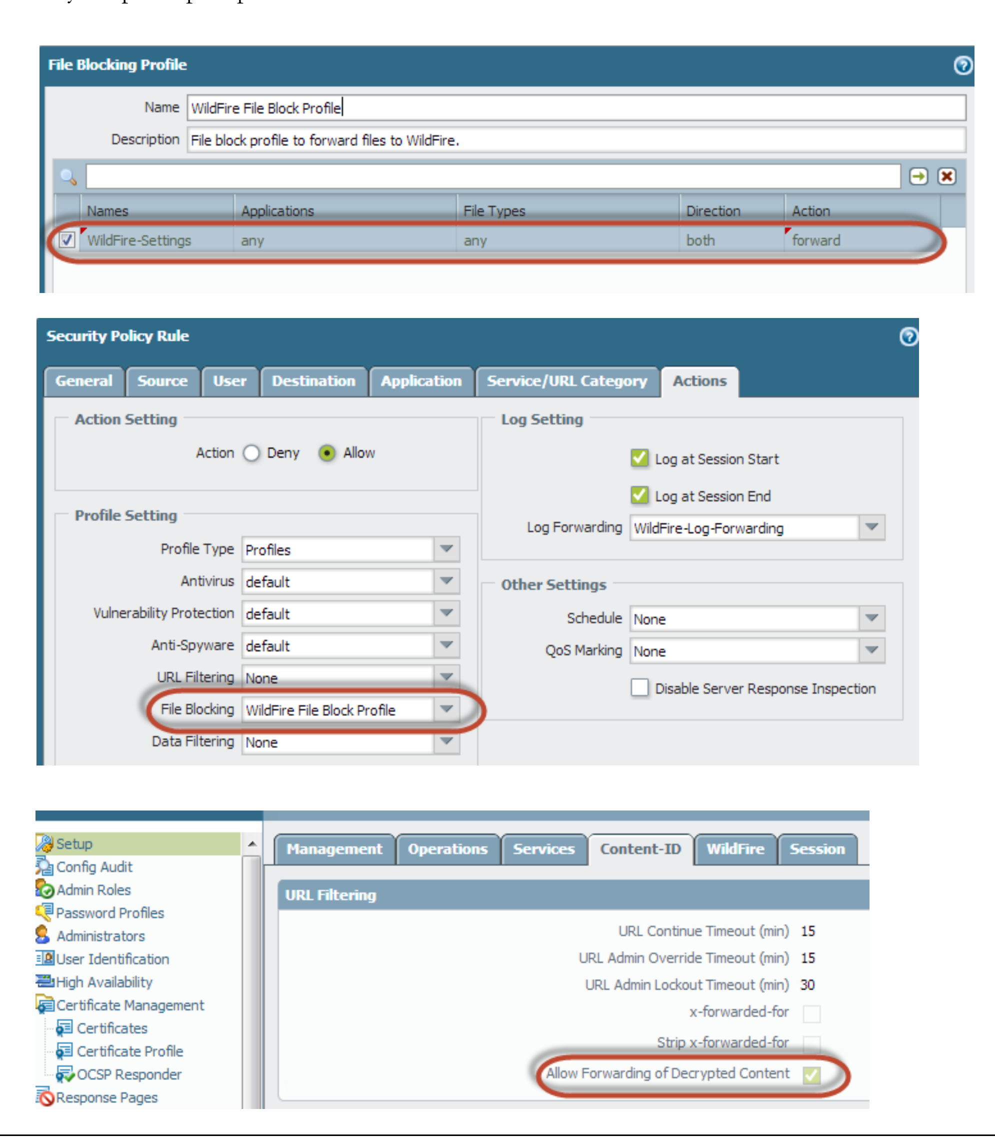
Si desea más información sobre la configuración de WildFire, consulte Envío de archivos a la nube de WildFire o Reenvío de archivos a un dispositivo WF-500 WildFire.



Este ejemplo usa un sitio web que utiliza cifrado SSL, por lo que el descifrado debe configurarse en el cortafuegos y la opción **Permitir reenvío de contenido descifrado** debe estar habilitada. Para obtener más información sobre la configuración del descifrado, consulte la *Palo Alto Networks Getting Started Guide (Guía de inicio de Palo Alto Networks)*. Para obtener información sobre cómo habilitar el reenvío de contenido descifrado, consulte Envío de archivos a la nube de WildFire o Reenvío de archivos a un dispositivo WF-500 WildFire.

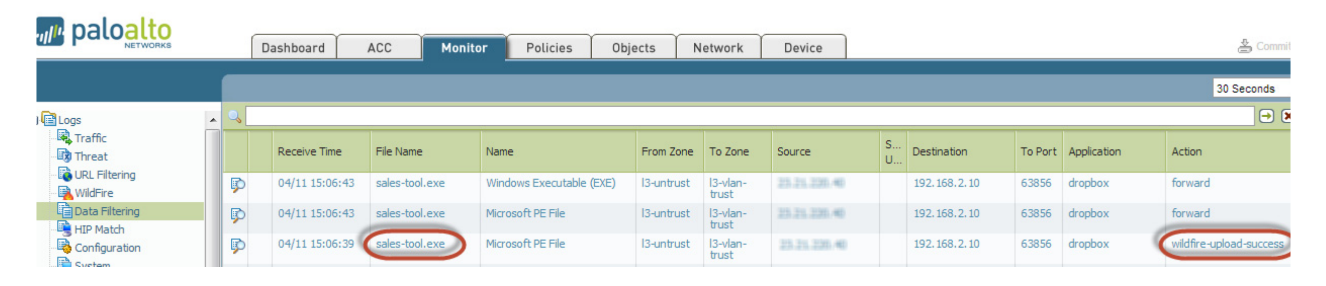
Caso de ejemplo de WildFire	
Paso 1	El representante de ventas de la empresa asociada carga un archivo de una herramienta de ventas denominado *sales-tool.exe* en su cuenta de Dropbox y, a continuación, envía un correo electrónico a la representante de ventas de Palo Alto Networks con un enlace al archivo.
Paso 2	La representante de ventas de Palo Alto recibe el correo electrónico del socio de ventas y hace clic en el enlace de descarga, que la lleva al sitio de Dropbox. A continuación, hace clic en **Descargar** y el archivo se guarda en su escritorio.  

Caso de ejemplo de WildFire (Continuación)
Paso 3 El cortafuegos que protege a la representante de ventas de Palo Alto tiene un perfil de bloqueo de archivos adjunto a una política de seguridad que busca archivos en cualquier aplicación utilizada para descargar o cargar cualquier tipo de archivo compatible (PE, PDF, APK, JAR/Class o MS Office). En cuanto la representante de ventas hace clic en Descargar, la política del cortafuegos también reenvía el archivo sales-tool.exe a WildFire, donde el archivo se analiza para comprobar si hay malware de día cero. Aun cuando la representante de ventas use Dropbox, que tiene cifrado SSL, el cortafuegos está configurado para descifrar tráfico, por lo que todo el tráfico se puede inspeccionar y los archivos se pueden reenviar a WildFire. Las siguientes capturas de pantalla muestran el perfil de bloqueo de archivos, la política de seguridad configurada con el perfil de bloqueo de archivos y la opción para permitir el reenvío de contenido descifrado.



Caso de ejemplo de WildFire (Continuación)

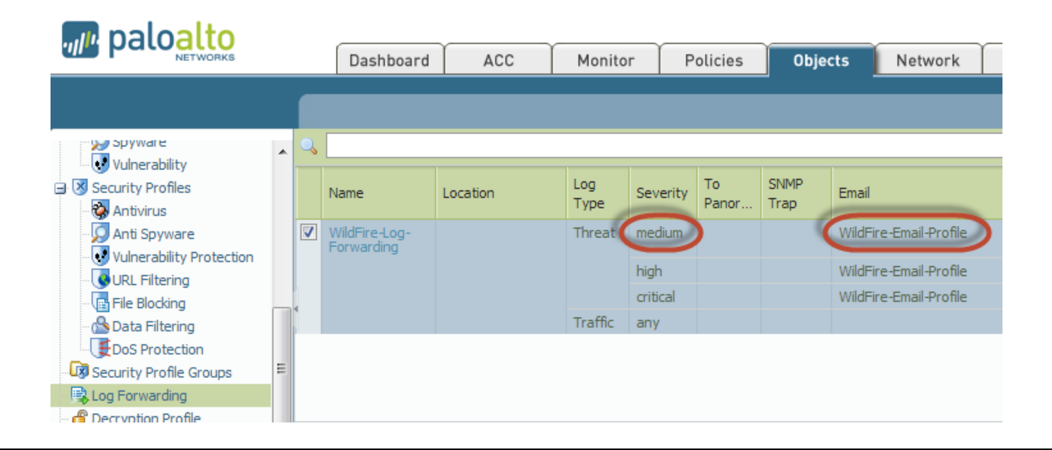
Paso 4 En este momento, WildFire ha recibido el archivo y está analizándolo en busca de más de 100 comportamientos malintencionados distintos. Para ver que el archivo se ha reenviado correctamente, consulte **Supervisar > Logs > Filtrado de datos** en el cortafuegos.



Paso 5 En aproximadamente cinco minutos, WildFire ha terminado el análisis del archivo y envía un log de WildFire al cortafuegos con los resultados del análisis. En este ejemplo, el log de WildFire muestra que el archivo es malintencionado.



Paso 6 También hay configurado un perfil de reenvío de registros para enviar por correo electrónico alertas de WildFire, de modo que el administrador de seguridad recibe inmediatamente un correo electrónico en relación con el malware que ha descargado.



Caso de ejemplo de WildFire (Continuación)

Paso 7 El administrador de seguridad identificará el usuario por el nombre si el ID de usuarios está configurado o, en caso contrario, por dirección IP. En este punto, el administrador puede apagar la red o la conexión VPN que está usando la representante de ventas y, a continuación, ponerse en contacto con el grupo de asistencia técnica para que ayude al usuario a comprobar y limpiar el sistema.

Al usar el informe de análisis detallado de WildFire, el técnico del grupo de asistencia técnica puede determinar si el sistema del usuario está infectado con malware examinando los archivos, los procesos y la información de registro detallados en el informe del análisis de WildFire. Si se ha ejecutado el malware, el técnico puede intentar limpiar el sistema manualmente o volver a crear una imagen de este.

Para obtener detalles de los campos del informe de WildFire, consulte ¿Qué contienen los informes de WildFire?.

Ilustración: Vista parcial del informe de análisis de WildFire en PDF

1 File Information

File Type	PE
File Signer	
SHA-256	bd93a2c673bf90a08bd9ff31f1c023da2d722d3c0ca5bb09462865580e7a41ac
MD5	d11931c7016a350cbf5e0da0352ae514
File Size	739884 bytes
First Seen Timestamp	2013-09-26 23:45:24 UTC
Verdict	Malware
Antivirus Coverage	VirusTotal Information

2 Dynamic Analysis

2.1. VM1 (Windows XP, Adobe Reader 9.4.0, Flash 10, Office 2007)

2.1.1. Behavioral Summary

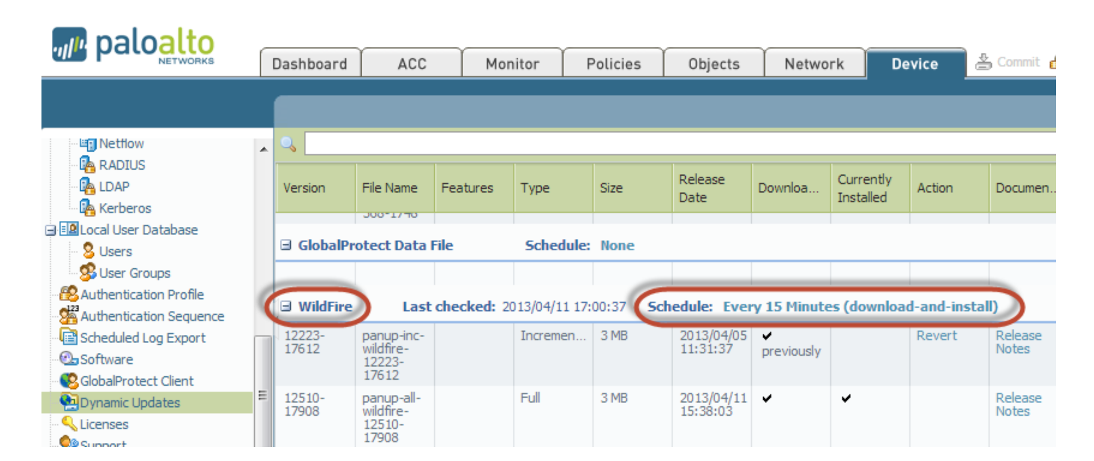
This sample was found to be **malware** on this virtual machine.

Behavior
Created a file in the Windows folder
Created or modified files
Installed a browser helper object
Spawned new processes
Modified Windows registries
Changed security settings of Internet Explorer
Created an executable file in a user document folder

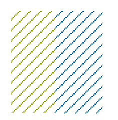
2.1.2. Network Activity

Caso de ejemplo de WildFire (Continuación)

Paso 8 Una vez identificado el malware y comprobado el sistema del usuario, ¿cómo protegerse frente a futuras exposiciones? La respuesta: En este ejemplo, el administrador ha definido una programación en el cortafuegos para descargar e instalar firmas de WildFire cada 15 minutos y para descargar e instalar actualizaciones del antivirus a diario. En menos de una hora y media, la representante de ventas ha descargado el archivo infectado, WildFire ha identificado el malware de día cero, ha generado una firma, la ha añadido a la base de datos de firmas de actualización de WildFire proporcionada por Palo Alto Networks y el cortafuegos ha descargado la nueva firma. Este cortafuegos y cualquier otro cortafuegos de Palo Alto Networks configurado para descargar firmas de WildFire y de amenazas ahora está protegido frente a este malware detectado recientemente. La siguiente captura de pantalla muestra la programación de actualizaciones de WildFire:



Todo esto tiene lugar mucho antes de que la mayoría de los proveedores de antivirus perciban incluso la existencia de malware de día cero. En este ejemplo, el malware ya no se considera de día cero, ya que Palo Alto Networks sabe de su existencia y ya ha proporcionado la protección correspondiente a sus clientes.



Referencia de la CLI del software del dispositivo WildFire

Esta sección describe los comandos de la CLI específicos para el software del dispositivo WF-500 WildFire. El resto de comandos, tales como las interfaces de configuración, confirmación de la configuración y el ajuste de la información del sistema, son idénticos a PAN-OS y también se muestran en la jerarquía. Para obtener más información sobre los comandos de PAN-OS, consulte la *Guía de referencia de la interfaz de línea de comandos de PAN-OS de Palo Alto Networks*.

▲ Acerca del software del dispositivo WildFire

▲ Comandos del modo de configuración

▲ Comandos del modo de operación

Acerca del software del dispositivo WildFire

En esta sección se presenta la interfaz de línea de comandos (CLI) del software del dispositivo WildFire y se describe su uso:

- ▲ Acerca de la estructura de la CLI del software del dispositivo WildFire
- ▲ Acceso a la CLI
- ▲ Uso de los comandos de la CLI del software del dispositivo WildFire

Acerca de la estructura de la CLI del software del dispositivo WildFire

La CLI del software del dispositivo WildFire se usa para manejar dicho dispositivo. La CLI es la única interfaz del dispositivo. Sirve para ver información de estado y configuración y modificar la configuración del dispositivo. Acceda a la CLI del software del dispositivo WildFire a través de SSH o de un acceso directo a la consola usando el puerto de la consola.

La CLI del software del dispositivo WildFire tiene dos modos de funcionamiento:

- **Modo de operación**: Permite ver el estado del sistema, navegar por la CLI del software del dispositivo WildFire y acceder al modo de configuración.
- **Modo de configuración**: Permite ver y modificar la jerarquía de configuración.

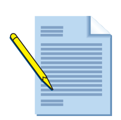
Si desea más información sobre estos modos, consulte Modos de comando de la CLI.

Acceso a la CLI

En esta sección se describe cómo acceder y comenzar a usar la CLI del software del dispositivo WildFire:

- ▲ Establecimiento de una conexión directa con la consola
- ▲ Establecimiento de una conexión de SSH

Establecimiento de una conexión directa con la consola



Consulte la *WF-500 WildFire Appliance Hardware Reference Guide (Guía de referencia de hardware de WF-500 WildFire)* para obtener información acerca de la instalación del hardware e Inicio rápido para información sobre configuración inicial del dispositivo.

Utilice la siguiente configuración en la conexión directa de la consola:

- Tasa de datos: 9600
- Bits de datos: 8
- Paridad: No
- Bits de terminación: 1
- Control de flujo: Ninguna

Establecimiento de una conexión de SSH

Para acceder a la CLI del software del dispositivo WildFire:

Paso 1 Abra la conexión de la consola.

Paso 2 Introduzca el nombre del usuario administrativo. El valor predeterminado es admin.

Paso 3 Introduzca la contraseña administrativa. El valor predeterminado es admin.

Paso 4 La CLI del software del dispositivo WildFire se abre en el modo de operación y se muestra el siguiente mensaje de la CLI:

```
username@hostname>
```

Uso de los comandos de la CLI del software del dispositivo WildFire

- ▲ Convenciones de comandos de la CLI del software del dispositivo WildFire
- ▲ Mensajes de comandos de la CLI
- ▲ Acceso a los modos de operación y configuración

- ▲ Mostrar opciones de comandos de la CLI del software del dispositivo WildFire
- ▲ Símbolos de opciones de comandos
- ▲ Niveles de privilegio
- ▲ Modos de comando de la CLI

Convenciones de comandos de la CLI del software del dispositivo WildFire

El mensaje de comandos básico incluye el nombre de usuario y de host del dispositivo:

```
username@hostname>
```

Ejemplo:

```
msimpson@wf-corp1>
```

Al entrar en el modo de configuración, el mensaje cambia de > a #:

```
username@hostname> (modo de operación)
username@hostname> configure
Entering configuration mode
[edit]
username@hostname> (modo de configuración)
```

En el modo de configuración, el contexto de jerarquía actual se muestra en el titular `[editar...]` que aparece entre corchetes cuando se emite un comando.

Mensajes de comandos de la CLI

Pueden aparecer mensajes al emitir un comando. Los mensajes ofrecen información de contexto y pueden ayudar a corregir comandos no válidos. En los siguientes ejemplos, el mensaje se muestra en negrita.

Ejemplo: Comando desconocido

```
username@hostname# application-group
Unknown command: application-group
[edit network]
username@hostname#
```

Ejemplo: Modos de cambio

```
username@hostname# exit
Exiting configuration mode
username@hostname>
```

Ejemplo: Sintaxis no válida

```
username@hostname> debug 17
Unrecognized command
Invalid syntax.
username@hostname>
```

La CLI comprueba la sintaxis de cada comando. Si la sintaxis es correcta, se ejecuta el comando y se registran los cambios de la jerarquía del candidato. Si la sintaxis no es correcta, aparece un mensaje de sintaxis no válida, como en el siguiente ejemplo:

```
username@hostname# set deviceconfig setting wildfire auto-submit yes
```

```
Unrecognized command
Invalid syntax.
[edit]
username@hostname#
```

Acceso a los modos de operación y configuración

Al iniciar sesión, la CLI del software del dispositivo WildFire se abre en el modo de operación. Puede alternar entre los modos de operación y navegación en cualquier momento.

- Para entrar en el modo de configuración desde el modo de operación, use el comando `configurar`:

```
username@hostname> configure
Entering configuration mode
[edit]
username@hostname#
```

- Para salir del modo de configuración y regresar al modo de operación, use el comando `abandonar` o el comando `salir`:

```
username@hostname# quit
Exiting configuration mode
username@hostname>
```

Para introducir un comando del modo de operación mientras está en el modo de configuración, use el comando `run`. Por ejemplo, para mostrar recursos del sistema desde el modo de configuración, use `run show system resources`.

Mostrar opciones de comandos de la CLI del software del dispositivo WildFire

Use `?` (o **Meta-H**) para mostrar una lista de opciones de comandos, basada en el contexto:

- Para mostrar una lista de comandos de operación, introduzca **?** en el mensaje del comando.

```
username@hostname> ?
  clear       Clear runtime parameters
  configure   Manipulate software configuration information
  debug       Debug and diagnose
  exit        Exit this session
  grep        Searches file for lines containing a pattern match
  less        Examine debug file content
  ping        Ping hosts and networks
  quit        Exit this session
  request     Make system-level requests
  scp         Use ssh to copy file to another host
  set         Set operational parameters
  show        Show operational parameters
  ssh         Start a secure shell to another host
  tail        Print the last 10 lines of debug file content
username@hostname>
```

- Para mostrar las opciones disponibles de un comando especificado, introduzca el comando seguido de **?**.

Ejemplo:

```
username@hostname> ping ?
+ bypass-routing      Bypass routing table, use specified interface
+ count               Number of requests to send (1..2000000000 packets)
+ do-not-fragment     Don't fragment echo request packets (IPv4)
+ inet                Force to IPv4 destination
+ interface           Source interface (multicast, all-ones, unrouted packets)
+ interval            Delay between requests (seconds)
+ no-resolve          Don't attempt to print addresses symbolically
+ pattern             Hexadecimal fill pattern
+ record-route        Record and report packet's path (IPv4)
+ size                Size of request packets (0..65468 bytes)
+ source              Source address of echo request
+ tos                 IP type-of-service value (0..255)
+ ttl                 IP time-to-live value (IPv6 hop-limit value) (0..255 hops)
+ verbose             Display detailed output
+ wait                Delay after sending last packet (seconds)
  <host>              Hostname or IP address of remote host
```

Símbolos de opciones de comandos

El símbolo que precede a una opción puede proporcionar información adicional acerca de la sintaxis de comandos.

Símbolo	Descripción
*	Esta opción es obligatoria.
>	Hay opciones adicionales anidadas para este comando.
+	Hay opciones de comando adicionales para este comando en este nivel.
|	Hay una opción para especificar un “valor de excepción” o un “valor de coincidencia” para restringir el comando.
“ ”	Aunque las comillas dobles no son un símbolo de opción de comando, deben usarse al introducir frases de varias palabras en comandos de CLI. Por ejemplo, para crear un nombre de grupo de dirección llamado Grupo de prueba y añadir el usuario llamado nombre1 a este grupo, debe escribir el nombre del grupo con comillas dobles alrededor del siguiente modo: establecer grupo de direcciones “Grupo de prueba” usuario1. Si no coloca comillas dobles alrededor del nombre del grupo, la CLI podría interpretar la palabra Prueba como el nombre del grupo y Grupo como el nombre de usuario y se mostraría el siguiente mensaje de error: “prueba no es un nombre válido”. Nota: Las comillas simples tampoco serían válidas en este ejemplo.

Los siguientes ejemplos muestran cómo se usan estos símbolos.

Ejemplo: En el siguiente comando, es obligatoria la palabra clave `from`:

```
username@hostname> scp import configuration ?
+ remote-port   SSH port number on remote host
* from          Source (username@host:path)
username@hostname> scp import configuration
Example: This command output shows options designated with + and >.
username@hostname# set rulebase security rules rule1 ?
+ action                 action
+ application            application
+ destination            destination
+ disabled               disabled
+ from                   from
+ log-end                log-end
+ log-setting            log-setting
+ log-start              log-start
+ negate-destination     negate-destination
+ negate-source          negate-source
+ schedule               schedule
+ service                service
+ source                 source
+ to                     to
> profiles               profiles
  <Enter>                Finish input
 [edit]
username@hostname# set rulebase security rules rule1
```

Cada opción de la lista marcada con + se puede añadir al comando.

La palabra clave perfiles (con >) tiene opciones adicionales:

```
username@hostname# set rulebase security rules rule1 profiles ?
+ virus             Help string for virus
+ spyware           Help string for spyware
+ vulnerability     Help string for vulnerability
+ group             Help string for group
  <Enter>           Finish input
 [editar]
username@hostname# set rulebase security rules rule1 profiles
```

Restricción de resultados de comandos

Algunos comandos de operación incluyen una opción para restringir el resultado que aparece. Para restringir el resultado, introduzca un símbolo de barra vertical seguido de `except` o `match` y el valor que se debe incluir o excluir:

Ejemplo:

El siguiente resultado de muestra pertenece al comando `mostrar información del sistema`:

```
username@hostname> show system info
hostname: wf-corp1
ip-address: 192.168.2.20
netmask: 255.255.255.0
default-gateway: 192.168.2.1
```

```
mac-address: 00:25:90:95:84:76
vm-interface-ip-address: 10.16.0.20
vm-interface-netmask: 255.255.252.0
vm-interface-default-gateway: 10.16.0.1
vm-interface-dns-server: 10.0.0.247
time: Mon Apr 15 13:31:39 2013
uptime: 0 days, 0:02:35
family: m
model: WF-500
serial: 009707000118
sw-version: 5.1.0
logdb-version: 5.0.2
platform-family: m

username@hostname>
```

El siguiente ejemplo muestra solo información del modelo del sistema:

```
username@hostname> show system info | match model
model: WF-500

username@hostname>
```

Niveles de privilegio

Los niveles de privilegio determinan los comandos que el usuario tiene permitido ejecutar y la información que el usuario tiene permitido ver.

Nivel	Descripción
superreader	Tiene solo acceso de lectura completo al dispositivo.
superuser	Tiene acceso de lectura-escritura completo al dispositivo.

Modos de comando de la CLI

Esta sección describe los modos usados para interactuar con la CLI del software del dispositivo WildFire:

- ▲ Acerca del modo de configuración
- ▲ Acerca del modo de operación

Acerca del modo de configuración

Al introducir comandos en el modo de configuración se modifica la configuración del candidato. La configuración del candidato modificada se almacena en la memoria del dispositivo y se conserva mientras el dispositivo esté en funcionamiento.

Cada comando de configuración implica una acción, y también puede incluir palabras clave, opciones y valores.

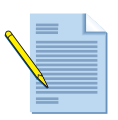
En esta sección se describen el modo de configuración y la jerarquía de configuración:

- ▲ Uso de comandos del modo de configuración
- ▲ Acerca de la jerarquía de configuración
- ▲ Navegación por la jerarquía

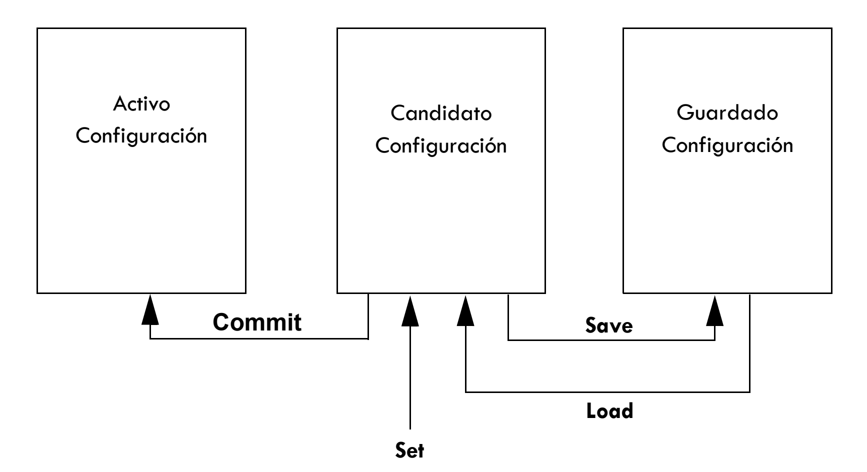
Uso de comandos del modo de configuración

Use los siguientes comandos para almacenar y aplicar cambios de configuración:

- `save`: Guarda la configuración del candidato en la memoria permanente del dispositivo. La configuración guardada se conserva hasta que se vuelva a usar el comando **guardar** para sobrescribirla. Tenga en cuenta que este comando no activa la configuración.
- `commit`: Aplica la configuración del candidato al dispositivo. Una configuración compilada vuelve activa la configuración del dispositivo.
- `set`: Cambia un valor en la configuración del candidato.
- `load`: Asigna la última configuración guardada o una configuración especificada para ser la configuración del candidato.



Cuando se cambia el modo de configuración sin emitir el comando save o commit, los cambios de configuración podrían perderse si se interrumpe la alimentación del dispositivo.



Mantener la configuración de un candidato y separar los pasos de guardado y compilación conlleva importantes ventajas en comparación con las arquitecturas CLI tradicionales:

- Distinguir entre los conceptos de **save** y **commit** permite hacer múltiples cambios simultáneos y reduce la vulnerabilidad del sistema.
- Los comandos se pueden adaptar fácilmente para funciones similares.
- Por ejemplo, al configurar dos interfaces Ethernet, cada una con una dirección IP, puede editar la configuración de la primera interfaz, copiar el comando, modificar solo la interfaz y la dirección IP y, a continuación, aplicar el cambio a la segunda interfaz.
- La estructura de comandos siempre es constante.

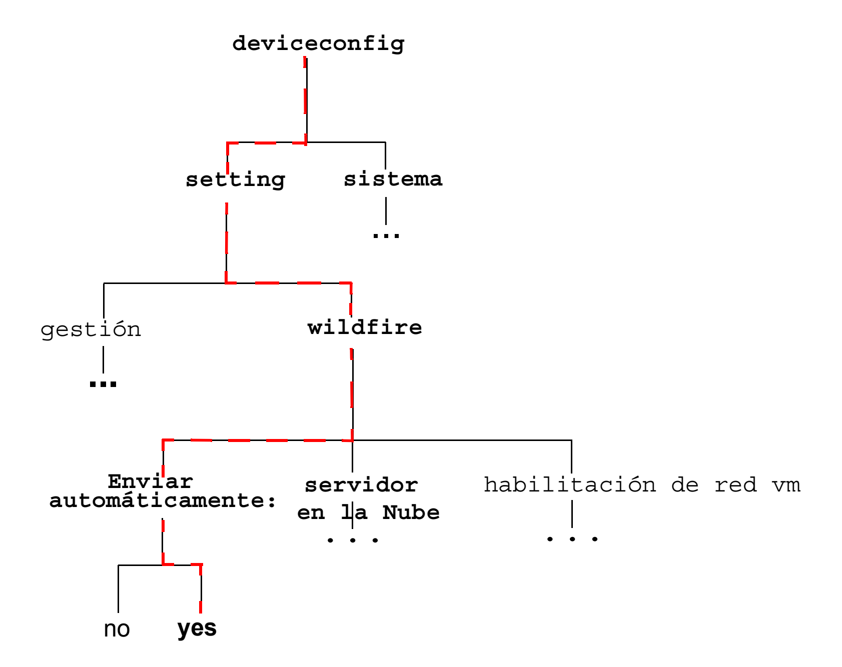
Dado que la configuración del candidato siempre es exclusiva, todos los cambios autorizados de la configuración del candidato serán coherentes entre sí.

Acerca de la jerarquía de configuración

La configuración del dispositivo se organiza con una estructura jerárquica. Para mostrar un segmento del nivel actual de la jerarquía, use el comando `show`. Al introducir mostrar, aparece la jerarquía completa, mientras que al introducir `show` con palabras clave, aparece un segmento de la jerarquía. Por ejemplo, cuando se ejecuta el comando `show` desde el nivel más alto del modo de configuración, se muestra toda la configuración. Si se ejecuta el comando `edit mgt-config` y se introduce `show`, o se ejecuta el comando **mostrar configuración de gestión**, solo aparece la parte de la jerarquía relativa a la configuración de gestión.

Rutas de jerarquía

Al introducir comandos, la ruta se traza a través de la jerarquía del siguiente modo:

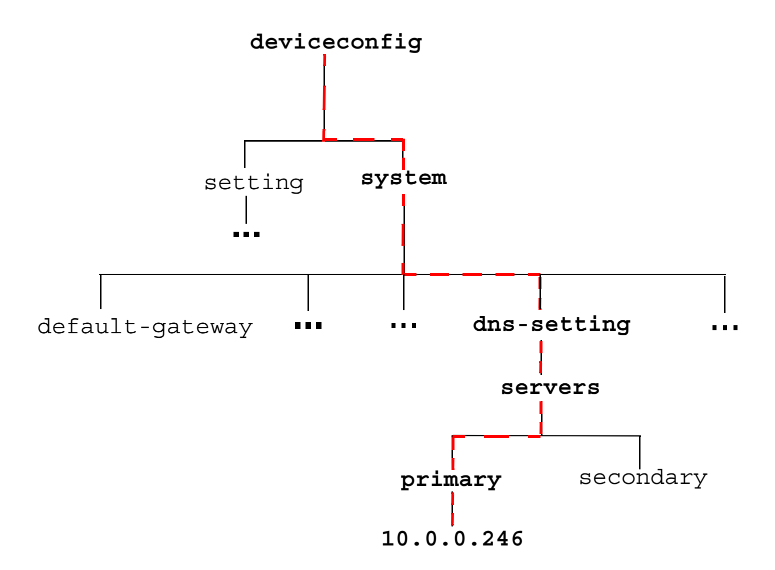


Por ejemplo, el siguiente comando asigna el servidor de DNS principal 10.0.0.246 para el dispositivo:

```
     [edit]
username@hostname# set deviceconfig system dns-setting servers primary
10.0.0.246
```

Este comando genera un nuevo elemento en la jerarquía y en los resultados del siguiente comando `show`:

```
[edit]
username@hostname# show deviceconfig system dns-settings
dns-setting {
    servers {
      primary 10.0.0.246
      }
  }
[edit]
username@hostname#
```



Navegación por la jerarquía

El titular [editar...] presentado a continuación de la línea del símbolo de sistema del modo de configuración muestra el contexto de jerarquía actual.

```
[editar]
```

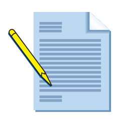
indica que el contexto relativo es el máximo nivel de la jerarquía, mientras que

```
[editar deviceconfig]
```

indica que el contexto relativo está al nivel de deviceconfig.

Use los comandos de la lista para navegar por la jerarquía de configuración.

Nivel	Descripción
edit	Establece el contexto para la configuración dentro de la jerarquía de comandos.
up	Cambia el contexto al nivel superior de la jerarquía.
top	Cambia el contexto al nivel más alto de la jerarquía.



Si se emite el comando `establecer` después de usar los comandos `up` y `top`, se inicia desde un nuevo contexto.

Acerca del modo de operación

La primera vez que se inicia sesión en el dispositivo, la CLI del software del dispositivo WildFire se abre en el modo de operación. Los comandos del modo de operación tienen que ver con acciones que se ejecutan inmediatamente. No suponen cambios en la configuración, y no es necesario guardarlos o compilarlos.

Los comandos del modo de operación son de diversos tipos:

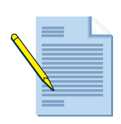
- **Acceso a la red**: Abre una ventana a otro host. Es compatible con SSH.
- **Supervisión y solución de problemas**: Realizar diagnósticos y análisis. Incluye los comandos **debug** y **ping**.
- **Mostrar comandos**: Muestra o borra la información actual. Incluye los comandos **clear** y **show**.
- **Comandos de navegación de la CLI del software del dispositivo WildFire**: Entrar en el modo de configuración o salir de la CLI del software del dispositivo WildFire. Incluye los comandos **configure**, **exit** y **quit**.
- **Comandos del sistema**: Hace solicitudes en el nivel del sistema o reinicia. Incluye los comandos **set** y **request**.

Establecimiento del formato de salida para comandos de configuración

Cambie el formato de salida para los comandos de configuración utilizando el comando `set cli config-output-format` en el modo de operación. Las opciones incluyen el formato predefinido, json (JavaScript Object Notation), formato establecido y formato XML. El formato predefinido es un formato jerárquico donde las secciones de configuración tienen sangría y están entre llaves.

Comandos del modo de configuración

Esta sección contiene información de consulta sobre comandos para los siguientes comandos del modo de configuración que son específicos del software del dispositivo WildFire. El resto de comandos que forman parte del software del dispositivo WildFire son idénticos a PAN-OS, consulte la *Guía de referencia de la interfaz de línea de comandos de PAN-OS de Palo Alto Networks* para obtener información sobre esos comandos.



Todos los comandos específicos de WildFire están en color azul en el resultado de la siguiente jerarquía y tienen un hiperenlace a la descripción.

```
deviceconfig {
  system {
    login-banner <value>;
    hostname <value>;
    domain <value>;
    speed-duplex
auto-negotiate|10Mbps-half-duplex|10Mbps-full-duplex|100Mbps-half-duplex|100Mbps-full-
duplex|
    1Gbps-full-duplex;
    ip-address <ip/netmask>;
    netmask <value>;
    default-gateway <ip/netmask>;
    vm-interface{
      ip-address <ip/netmask>;
      netmask <value>;
      default-gateway <ip/netmask>;
      mtu 576-1500;
      speed-duplex
      auto-negotiate|10Mbps-half-duplex|10Mbps-full-duplex|100Mbps-half-duplex|100Mbps
     -full-duplex|
      1Gbps-full-duplex;
      link-state up|down;
      dns-server <ip/netmask>;
    }
    geo-location {
      latitude <float>;
      longitude <float>;
    }
    timezone
    dns-setting {
        servers {
          primary <ip/netmask>;
          secondary <ip/netmask>;
        }
    }
    ntp-server-1 <value>;
    ntp-server-2 <value>;
    update-server <value>;
    secure-proxy-server <value>;
    secure-proxy-port 1-65535;
```

```
    secure-proxy-user <value>;
    secure-proxy-password <value>;
    service {
      disable-ssh yes|no;
      disable-icmp yes|no;
    }
  }
  setting {
    wildfire {
      active-vm;
      auto-submit yes|no;
      cloud-server <value>;
      vm-network-enable yes|no;
      vm-network-use-tor;
    }
    management {
      admin-lockout {
        failed-attempts 0-10;
        lockout-time 0-60;
      }
      idle-timeout 1-1440;
    }
  }
}

mgt-config {
  users {
    REPEAT...
    <name> {
      phash <value>;
      permissions {
        role-based {
          superreader yes;
          OR...
          superuser yes;
        }
      }
    }
  }
}

predefined;

shared {
  log-settings {
    system {
      informational {
        send-syslog {
          using-syslog-setting <value>;
        }
      }
      low {
```

```
        send-syslog {
          using-syslog-setting <value>;
        }
      }
      medium {
        send-syslog {
          using-syslog-setting <value>;
        }
      }
      high {
        send-syslog {
          using-syslog-setting <value>;
        }
      }
      critical {
        send-syslog {
          using-syslog-setting <value>;
        }
      }
    }
    config {
      any {
        send-syslog {
          using-syslog-setting <value>;
        }
      }
    }
    syslog {
      REPEAT...
      <name> {
        server {
          REPEAT...
          <name> {
            server <value>;
            port 1-65535;
            facility
LOG_USER|LOG_LOCAL0|LOG_LOCAL1|LOG_LOCAL2|LOG_LOCAL3|LOG_LOCAL4|LOG_LOCAL5|LOG_LOCAL6|
LOG_LOCAL7;
          }
        }
      }
    }
  }
}
```

interfaz vm

Descripción

La interfaz vm sirve para permitir que el software malintencionado que se ejecuta en las máquinas virtuales de WildFire acceda a Internet para habilitar análisis de archivos más exhaustivos. Se recomienda la activación de este puerto, que a su vez ayudará a WildFire a identificar mejor la actividad maliciosa si el software malintencionado accede a Internet para phone-home u otra actividad. Es importante que esta interfaz esté en una red aislada para Internet. Para obtener más información acerca de la interfaz vm, consulte Configuración de interfaz de la máquina virtual.

Tras configurar la interfaz vm, habilítela ejecutando el siguiente comando:

```
set deviceconfig setting wildfire vm-network-enable yes
```

Ubicación de jerarquía

```
set deviceconfig system
```

Sintaxis

```
set vm-interface {
  ip-address <ip_address>;
  netmask <ip_address>;
  default-gateway <ip_address>;
  dns-server <ip_address>;
```

Opciones

```
admin@wf-corp1# establecer interfaz vm
+ default-gateway   Default gateway
+ dns-server        dns server
+ ip-address        IP address for wildfire vm download interface
+ link-state        Link state up or down
+ mtu               Maximum Transmission Unit for the management interface
+ netmask           IP netmask for wildfire vm download interface
+ speed-duplex      Speed and duplex for wildfire vm download interface
```

Resultado de muestra

A continuación se muestra una interfaz vm configurada.

```
vm-interface {
  ip-address 10.16.0.20;
  netmask 255.255.252.0;
  default-gateway 10.16.0.1;
  dns-server 10.0.0.246;
}
```

Nivel de privilegios requerido

```
superuser, superreader
```

wildfire

Descripción

Configure los ajustes de Wildfire para que envía automáticamente el software malintencionado a la Nube de Palo Alto Networks WildFire para generar firmas, definir el servidor de la Nube que recibirá los archivos infectados por software malintencionado y habilitar o deshabilitar la interfaz vm. Lea la descripción de la interfaz vm antes de habilitarla.

Ubicación de jerarquía

```
set deviceconfig settings
```

Sintaxis

```
wildfire {
      active-vm;
      auto-submit yes|no;
      cloud-server <value>;
      vm-network-enable yes|no;
      vm-network-use-tor;
    }
```

Opciones

```
admin@wf-corp1# establecer wildfire
+ active-vm shows the virtual machine environment that is currently selected. Each vm
has a different configuration, such as Windows XP, versions of Flash, Adobe reader, etc.
To view which VM is selected, run show wildfire status from operational mode.
+ auto-submit automatically submit all malwares/incorrect verdict to public cloud
+ cloud-server Hostname for cloud server. Default is wildfire-public-cloud
+ vm-network-enable enable/disable is used to enable the vm-network, which is enable
internet access to sample files running in the virtual machine sandbox. This helps
WildFire analyze the behavior of the malware.
+ vm-network-use-tor enable/disable is used to enable the Tor network for the
vm-interface. When this option is enabled, any malicious traffic coming from the
sandbox systems on the WF-500 during sample analysis will be sent through the Tor
network. The Tor network will mask your public facing IP address, so the owners of the
malicious site cannot determine the source of the traffic.
```

Resultado de muestra

El siguiente resultado muestra que el envío automático no está habilitado en el dispositivo WildFire, de modo que los archivos infectados por software malintencionado no se enviarán a la Nube de WildFire. Si el envío automático estuviera habilitado, se enviarían los archivos a la Nube de WildFire porque el servidor de la Nube de la Nube pública de wildfire está definido. También muestra que la interfaz vm está habilitada, lo cual permitirá que el software malintencionado que se ejecuta en máquinas virtuales de WildFire accedan a Internet.

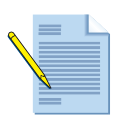
```
wildfire {
  active-vm vm-1;
  auto-submit no;
  cloud-server wildfire-public-cloud;
  vm-network-enable yes;
  vm-network-use-tor no;
}
```

Nivel de privilegios requerido

superuser, superreader

Comandos del modo de operación

Esta sección contiene información de consulta sobre comandos para los siguientes comandos del modo de operación que son específicos del software del dispositivo WildFire. El resto de comandos que forman parte del software del dispositivo WildFire son idénticos a PAN-OS, consulte la *Guía de referencia de la línea de comandos de PAN-OS de Palo Alto Networks* para obtener información sobre esos comandos.



Todos los comandos específicos de WildFire de la siguiente jerarquía tienen un hiperenlace a la descripción.

```
test {
  wildfire {
    registration;
  }
}
set {
  wildfire {
portal-admin {
      password <value>;
    }
  }
  OR...
  management-server {
    unlock {
      admin <value>;
    }
    OR...
    logging on|off|import-start|import-end;
  }
  OR...
  password;
  OR...
  ssh-authentication {
    public-key <value>;
  }
  OR...
  cli {
    config-output-format default|xml|set|json;
    OR...
    pager on|off;
    OR...
    confirmation-prompt on|off;
    OR...
    scripting-mode on|off;
    OR...
    timeout {
      idle 1-1440;
    }
    OR...
```

```
    hide-ip;
    OR...
    hide-user;
  }
  OR...
  clock {
    date <value>;
    time <value>;
  }
}

request {
  system {
    software {
      info;
      OR...
      check;
      OR...
      download {
        version <value>;
        OR...
        file <value>;
      }
      OR...
      install {
          version <value>;
          OR...
          file <value>;
        load-config <value>;
      }
    }
    OR...
    raid {
      remove <value>;
      OR...
      copy {
        from <value>;
        to <value>;
      }
      OR...
      add {
        REPEAT...
        <name> {
          force {
            no-format;
          }
        }
      }
    }
  }
  OR...
  password-hash {
```

```
    password <value>;
    username <value>;
  }
  OR...
  commit-lock {
    add {
      comment <value>;
    }
    OR...
    remove {
      admin <value>;
    }
  }
  OR...
  config-lock {
    add {
      comment <value>;
    }
    OR...
    remove;
  }
  OR...
  tech-support {
    dump;
  }
  OR...
  stats {
    dump;
  }
  OR...
  shutdown {
    system;
  }
  OR...
  system {
    software {
      info;
      OR...
      check;
      OR...
      download {
        version <value>;
        OR...
        file <value>;
      }
      OR...
      install {
          version <value>;
          OR...
          file <value>;
        load-config <value>;
      }
```

```
    }
  }
  OR...
  license {
    info;
    OR...
    fetch {
      auth-code <value>;
    }
    OR...
    install <value>;
  }
  OR...
  restart {
    system;
    OR...
    software;
  }
  OR...
  support {
    info;
    OR...
    check;
  }
}

check {
  pending-changes;
  OR...
  data-access-passwd {
    system;
  }
}

save {
  config {
    to <value>;
  }
}

load {
  config {
    key <value>;
      last-saved;
      OR...
      from <value>;
      OR...
      version <value>1-1048576;
      OR...
      partial {
        from <value>;
        from-xpath <value>;
```

```
        to-xpath <value>;
        mode merge|replace|append;
      }
  }
  OR...
  device-state;
}

load {
  config {
    key <value>;
      last-saved;
      OR...
      from <value>;
      OR...
      version <value>;
      OR...
      partial {
        from <value>;
        from-xpath <value>;
        to-xpath <value>;
        mode merge|replace|append;
      }
      OR...
      repo {
        device <value>;
          file <value>;
          OR...
          version <value>;
      }
  }
}

delete {
  config {
    saved <value>;
    OR...
    repo {
      device <value>;
        file <value>;
        OR...
        running-config;
    }
  }
  OR...
  software {
    image <value>;
    OR...
    version <value>;
  }
}
```

```
clear {
  job {
    id 0-4294967295;
  }
  OR...
  log {
    config;
    OR...
    system;
  }
  OR...
  counter {
    device;
  }
}

show {
  arp management|ethernet1/1|ethernet1/2|all;
  OR...
  neighbor management|ethernet1/1|ethernet1/2|all;
  OR...
  web-server {
    log-level;
  }
  OR...
  config {
    diff;
    OR...
    running {
      xpath <value>;
    }
    OR...
    candidate;
  }
  OR...
  interface management|ethernet1/1;
  OR...
  management-clients;
  OR...
  counter {
    management-server;
    OR...
    interface management|ethernet1/1;
    OR...
    device;
  }
  OR...
  ntp;
  OR...
  clock;
  OR...
wildfire {
```

```
    sample-status {
      sha256 {
        equal <value>;
      }
    }
    OR...
    status;
    OR...
    statistics;
    OR...
    latest {
      analysis {
        filter malicious|benign;
        sort-by SHA256|Submit Time|Start Time|Finish Time|Malicious|Status;
        sort-direction asc|desc;
        limit 1-20000;
        days 1-7;
      }
      OR...
      sessions {
        filter malicious|benign;
        sort-by SHA256|Create Time|Src IP|Src Port|Dst Ip|Dst Port|File|Device
        ID|App|Malicious|Status;
        sort-direction asc|desc;
        limit 1-20000;
        days 1-7;
      }
      OR...
      samples {
        filter malicious|benign;
        sort-by SHA256|Create Time|File Name|File Type|File Size|Malicious|Status;
        sort-direction asc|desc;
        limit 1-20000;
        days 1-7;
      }
      OR...
      uploads {
        sort-by SHA256|Create Time|Finish Time|Status;
        sort-direction asc|desc;
        limit 1-20000;
        days 1-7;
      }
    }
    OR...
    last-device-registration {
      all;
    }
  }
  OR...

  cli {
    info;
```

```
    OR...
    idle-timeout;
    OR...
    hide-ip;
    OR...
    hide-user;
    OR...
    permissions;
  }
  OR...
  jobs {
    all;
    OR...
    pending;
    OR...
    processed;
    OR...
    id 1-4294967296;
  }
  OR...
  location {
    ip <ip/netmask>;
  }
  OR...
  system {
    software {
      status;
    }
    OR...
    masterkey-properties;
    OR...
    info;
    OR...
    resources {
      follow;
    }
    OR...
    raid {
        detail;
    }
    OR...
    disk-space;
    OR...
    disk-partition;
    OR...
    files;
    OR...
    state {
        filter <value>;
        OR...
        filter-pretty <value>;
        OR...
```

```
        browser;
    }
    OR...
    environmentals {
        fans;
        OR...
        thermal;
        OR...
        power;
    }
    OR...
    setting {
      multi-vsys;
    }
  }
  OR...
  high-availability {
    all;
    OR...
    state;
    OR...
    control-link {
      statistics;
    }
    OR...
    transitions;
    OR...
    path-monitoring;
    OR...
    local-state;
  }
  OR...
  log {
    config {
      direction {
        equal forward|backward;
      }
      csv-output {
        equal yes|no;
      }
      query {
        equal <value>;
      }
      receive_time {
        in
last-60-seconds|last-15-minutes|last-hour|last-6-hrs|last-12-hrs|last-24-hrs|last-cale
ndar-day|last-7-days|last-30-days|last-calendar-month;
      }
      start-time {
        equal <value>;
      }
      end-time {
```

```
        equal <value>;
      }
      serial {
        equal <value>;
        OR...
        not-equal <value>;
      }
      client {
        equal web|cli;
        OR...
        not-equal web|cli;
      }
      cmd {
        equal
add|clone|commit|create|delete|edit|get|load-from-disk|move|rename|save-to-disk|set;
        OR...
        not-equal
add|clone|commit|create|delete|edit|get|load-from-disk|move|rename|save-to-disk|set;
      }
      result {
        equal succeeded|failed|unauthorized;
        OR...
        not-equal succeeded|failed|unauthorized;
      }
    }
    OR...
    system {
      direction {
        equal forward|backward;
      }
      csv-output {
        equal yes|no;
      }
      query {
        equal <value>;
      }
      receive_time {
        in
last-60-seconds|last-15-minutes|last-hour|last-6-hrs|last-12-hrs|last-24-hrs|last-cale
ndar-day|last-7-days|last-30-days|last-calendar-month;
      }
      start-time {
        equal <value>;
      }
      end-time {
        equal <value>;
      }
      serial {
        equal <value>;
        OR...
        not-equal <value>;
      }
      opaque {
```

```
        contains <value>;
      }
      severity {
        equal critical|high|medium|low|informational;
        OR...
        not-equal critical|high|medium|low|informational;
        OR...
        greater-than-or-equal critical|high|medium|low|informational;
        OR...
        less-than-or-equal critical|high|medium|low|informational;
      }
      subtype {
        equal <value>;
        OR...
        not-equal <value>;
      }
      object {
        equal <value>;
        OR...
        not-equal <value>;
      }
      eventid {
        equal <value>;
        OR...
        not-equal <value>;
      }
      id {
        equal <value>;
        OR...
        not-equal <value>;
      }
    }
  }
}

debug {
  web-server {
    reset-cache;
    OR...
    log-level {
      info;
      OR...
      warn;
      OR...
      crit;
      OR...
      debug;
    }
  }
  OR...
  delete {
    sample {
```

```
      sha256 {
        equal <value>;
      }
    }
  }
  OR...
  swm {
    list;
    OR...
    log;
    OR...
    history;
    OR...
    status;
    OR...
    unlock;
    OR...
    revert;
  }
  OR...
  tac-login {
      permanently-disable;
      OR...
      challenge;
      OR...
      response;
  }
  OR...
  software {
    restart {
      management-server;
      OR...
      web-server;
      OR...
      ntp;
    }
    OR...
    core {
      management-server;
      OR...
      web-server;
    }
    OR...
    trace {
      management-server;
      OR...
      web-server;
    }
  }
  OR...
  cli on|off|detail|show;
  OR...
```

```
system {
  maintenance-mode;
  OR...
  disk-sync;
  OR...
  ssh-key-reset {
    management;
    OR...
    all;
  }
}
OR...
device {
  set queue|all;
  OR...
  unset queue|all;
  OR...
  on error|warning|info|debug|dump;
  OR...
  off;
  OR...
  show;
  OR...
  clear;
  OR...
  dump {
    queues;
    OR...
    queue-stats;
    OR...
    queue <value>;
  }
  OR...
  flush {
    queue <value>;
  }
  OR...
  set-watermark {
    queue <value>;
    type high|low;
    value 0-4000;
  }
}
OR...
vardata-receiver {
  set {
    third-party libcurl|all;
    OR...
    all;
  }
  OR...
  unset {
```

```
    third-party libcurl|all;
    OR...
    all;
  }
  OR...
  on normal|debug|dump;
  OR...
  off;
  OR...
  show;
  OR...
  statistics;
}
OR...
wildfire {
  reset {
    forwarding;
  }
}
OR...
management-server {
  client {
    disable authd|useridd|ha_agent;
    OR...
    enable authd|useridd|ha_agent;
  }
  OR...
  conn;
  OR...
  on error|warn|info|debug|dump;
  OR...
  off;
  OR...
  clear;
  OR...
  show;
  OR...
  set {
    all;
    OR...
    comm basic|detail|all;
    OR...
    panorama basic|detail|all;
    OR...
    proxy basic|detail|all;
    OR...
    server basic|detail|all;
  }
  OR...
  unset {
    all;
    OR...
```

```
      comm basic|detail|all;
      OR...
      panorama basic|detail|all;
      OR...
      proxy basic|detail|all;
      OR...
      server basic|detail|all;
    }
  }
}

upload {
  generic_chunks {
    todir <value>;
    tofile <value>;
    offset 0-419430600;
    endoffile yes|no;
    content <value>;
  }
  OR...
  generic {
    name <value>;
    path <value>;
    content <value>;
    todir <value>;
    tofile <value>;
  }
  OR...
  config {
    name <value>;
    path <value>;
    content <value>;
  }
  OR...
  software {
    name <value>;
    path <value>;
    content <value>;
  }
  OR...
  license {
    name <value>;
    path <value>;
    content <value>;
  }
  OR...
  certificate {
    name <value>;
    passphrase <value>;
    path <value>;
    content <value>;
    certificate-name <value>;
```

```
  format pkcs12|pem;
}
OR...
private-key {
  name <value>;
  passphrase <value>;
  path <value>;
  content <value>;
  certificate-name <value>;
  format pkcs12|pem;
}
OR...
keypair {
  name <value>;
  passphrase <value>;
  path <value>;
  content <value>;
  certificate-name <value>;
  format pkcs12|pem;
}
OR...
ssl-optout-text {
  name <value>;
  path <value>;
  content <value>;
}
OR...
ssl-cert-status-page {
  name <value>;
  path <value>;
  content <value>;
}
OR...
logo {
  name <value>;
  path <value>;
  content <value>;
}
OR...
custom-logo {
    login-screen {
      name <value>;
      path <value>;
    }
    OR...
    main-ui {
      name <value>;
      path <value>;
    }
    OR...
    pdf-report-header {
      name <value>;
```

```
        path <value>;
      }
      OR...
      pdf-report-footer {
        name <value>;
        path <value>;
      }
  }
}

download {
  certificate {
    certificate-name <value>;
    include-key yes|no;
    format pem|pkcs12;
    passphrase <value>;
  }
  OR...
  csv;
  OR...
  techsupport;
  OR...
  statsdump;
  OR...
  generic {
    file <value>;
  }
}

scp {
  import {
    configuration {
      from <value>;
      remote-port 1-65535;
      source-ip <ip/netmask>;
    }
    OR...
    license {
      from <value>;
      remote-port 1-65535;
      source-ip <ip/netmask>;
    }
    OR...
    software {
      from <value>;
      remote-port 1-65535;
      source-ip <ip/netmask>;
    }
  }
  OR...
  export {
    mgmt-pcap {
```

```
      from <value>;
      to <value>;
      remote-port 1-65535;
      source-ip <ip/netmask>;
    }
    OR...
    configuration {
      from <value>;
      to <value>;
      remote-port 1-65535;
      source-ip <ip/netmask>;
    }
    OR...
    tech-support {
      to <value>;
      remote-port 1-65535;
      source-ip <ip/netmask>;
    }
  }
}

tftp {
  import {
    configuration {
      from <value>;
      file <value>;
      remote-port 1-65535;
      source-ip <ip/netmask>;
    }
    OR...
    certificate {
      from <value>;
      file <value>;
      remote-port 1-65535;
      source-ip <ip/netmask>;
      certificate-name <value>;
      passphrase <value>;
      format pkcs12|pem;
    }
    OR...
    private-key {
      from <value>;
      file <value>;
      remote-port 1-65535;
      source-ip <ip/netmask>;
      passphrase <value>;
      certificate-name <value>;
      format pkcs12|pem;
    }
    OR...
    keypair {
      from <value>;
```

```
      file <value>;
      remote-port 1-65535;
      source-ip <ip/netmask>;
      passphrase <value>;
      certificate-name <value>;
      format pkcs12|pem;
    }
    OR...
    license {
      from <value>;
      file <value>;
      remote-port 1-65535;
      source-ip <ip/netmask>;
    }
    OR...
    software {
      from <value>;
      file <value>;
      remote-port 1-65535;
      source-ip <ip/netmask>;
    }
  }
  OR...
  export {
    config-bundle {
      to <value>;
      remote-port 1-65535;
      source-ip <ip/netmask>;
    }
    OR...
    core-file {
      control-plane {
        from <value>;
        to <value>;
        remote-port 1-65535;
        source-ip <ip/netmask>;
      }
    }
    OR...
    device-state {
      to <value>;
      remote-port 1-65535;
      source-ip <ip/netmask>;
    }
    OR...
    mgmt-pcap {
      from <value>;
      to <value>;
      remote-port 1-65535;
      source-ip <ip/netmask>;
    }
    OR...
```

```
    configuration {
      from <value>;
      to <value>;
      remote-port 1-65535;
      source-ip <ip/netmask>;
    }
    OR...
    tech-support {
      to <value>;
      remote-port 1-65535;
      source-ip <ip/netmask>;
    }
    OR...
    log-file {
      management-plane {
        to <value>;
        remote-port 1-65535;
        source-ip <ip/netmask>;
      }
    }
  }
}

load {
  config {
    key <value>;
      last-saved;
      OR...
      from <value>;
      OR...
      version <value>1-1048576;
      OR...
      partial {
        from <value>;
        from-xpath <value>;
        to-xpath <value>;
        mode merge|replace|append;
      }
  }
  OR...
  device-state;
}

less {
    mp-log <value>;
    OR...
    mp-backtrace <value>;
}

grep {
  invert-match yes|no;
  line-number yes|no;
```

```
  ignore-case yes|no;
  no-filename yes|no;
  count yes|no;
  max-count 1-65535;
  context 1-65535;
  before-context 1-65535;
  after-context 1-65535;
  pattern <value>;
    mp-log <value>;
    OR...
    dp-log <value>;
}

tail {
  follow yes|no;
  lines 1-65535;
    mp-log <value>;
}

ssh {
  inet yes|no;
  port 0-65535;
  source <value>;
  v1 yes|no;
  v2 yes|no;
  host <value>;
}

telnet {
  8bit yes|no;
  port 0-65535;
  host <value>;
}

traceroute {
  ipv4 yes|no;
  first-ttl 1-255;
  max-ttl 1-255;
  port 1-65535;
  tos 1-255;
  wait 1-99999;
  pause 1-2000000000;
  do-not-fragment yes|no;
  debug-socket yes|no;
  gateway <ip/netmask>;
  no-resolve yes|no;
  bypass-routing yes|no;
  source <value>;
  host <value>;
}

netstat {
```

```
  route yes|no;
  interfaces yes|no;
  groups yes|no;
  statistics yes|no;
  verbose yes|no;
  numeric yes|no;
  numeric-hosts yes|no;
  numeric-ports yes|no;
  numeric-users yes|no;
  symbolic yes|no;
  extend yes|no;
  programs yes|no;
  continuous yes|no;
  listening yes|no;
  all yes|no;
  timers yes|no;
  fib yes|no;
  cache yes|no;
}

ping {
  bypass-routing yes|no;
  count 1-2000000000;
  do-not-fragment yes|no;
  interval 1-2000000000;
  source <value>;
  no-resolve yes|no;
  pattern <value>;
  size 0-65468;
  tos 1-255;
  ttl 1-255;
  verbose yes|no;
  host <value>;
}
```

test wildfire registration

Descripción

Ejecute una prueba para verificar si se han registrado correctamente el dispositivo WildFire o un cortafuegos con un servidor WildFire. Si la prueba es satisfactoria, se mostrarán la dirección IP o el nombre del servidor WildFire, lo que indica que el dispositivo/cortafuegos podrán enviar archivos al servidor de WildFire para su análisis.

Ubicación de jerarquía

Nivel máximo del modo de operaciones.

Sintaxis

```
test {
  wildfire {
    registration;
  }
}
```

Opciones

No hay opciones adicionales.

Resultado de muestra

A continuación se muestra un resultado satisfactorio de un cortafuegos que puede comunicarse con un dispositivo WildFire. Si es un dispositivo WildFire apuntando a la Nube de WildFire de Palo Alto Networks, el nombre del servidor de uno de los servidores de la Nube se muestra en el campo `select the best server:`

```
Test wildfire
        wildfire registration:        successful
        download server list:         successful
        select the best server:       ca-s1.wildfire.paloaltonetworks.com
```

Nivel de privilegios requerido

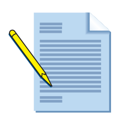
`superuser, superreader`

set wildfire portal-admin

Descripción

Establece la contraseña de la cuenta de administrador del portal que servirá para ver los informes de WildFire desde un cortafuegos. El nombre de usuario y la contraseña predeterminados son admin/admin. Tras introducir el comando, pulse Intro y aparecerá un mensaje para cambiar la contraseña.

Esta cuenta se usa cuando se ven los detalles del log de WildFire en el cortafuegos o Panorama y se hace clic en **Ver informe WildFire**. Después de la autenticación, se recupera el informe de análisis detallado de WildFire y se muestra en su explorador.



La cuenta de administrador del portal es la única cuenta para ver informes desde los logs; es posible cambiar la contraseña, pero no se puede cambiar el nombre de cuenta ni crear cuentas adicionales.

Ubicación de jerarquía

Nivel máximo del modo de operaciones.

Sintaxis

```
set {
  wildfire {
    portal-admin {
      password <value>;
    }
  }
```

Opciones

No hay opciones adicionales.

Resultado de muestra

A continuación se muestra el resultado de este comando.

```
admin@wf-corp1> set wildfire portal-admin password
Enter password   :
Confirm password :
```

Nivel de privilegios requerido

```
superuser, superreader
```

raid

Descripción

Use esta opción para manejar los pares de RAID instalados en el dispositivo WildFire. El dispositivo WF-500 WildFire se entrega con cuatro unidades en las cuatro primeras bahías de unidades (A1, A2, B1, B2). Las unidades A1 y A2 son el par RAID 1 y las unidades B1 y B2 son el segundo par RAID 1.

Ubicación de jerarquía

request system

Sintaxis

```
raid {
      remove <value>;
      OR...
      copy {
        from <value>;
        to <value>;
      }
      OR...
        add {
```

Opciones

```
> add      Add a drive into the corresponding RAID Disk Pair
> copy     Copy and migrate from one drive to other drive in the bay
> remove   drive to remove from RAID Disk Pair
```

Resultado de muestra

El siguiente resultado muestra un dispositivo WildFire WF-500 con una RAID configurada correctamente.

```
admin@wf-corp1> show system raid

Disk Pair A                           Available
   Disk id A1                           Present
   Disk id A2                           Present
Disk Pair B                           Available
   Disk id B1                           Present
   Disk id B2                           Present
```

Nivel de privilegios requerido

superuser, superreader

show wildfire

Descripción

Muestra la información de registro del dispositivo WildFire, actividad, muestras recientes que se han analizado e información de la máquina virtual.

Ubicación de jerarquía

```
show wildfire
```

Sintaxis

```
sample-status {
      sha256 {
        equal <value>;
      }
    }
    OR...
    status;
    OR...
    statistics;
    OR...
    latest {
      analysis {
        filter malicious|benign;
        sort-by SHA256|Submit Time|Start Time|Finish Time|Malicious|Status;
        sort-direction asc|desc;
        limit 1-20000;
        days 1-7;
      }
      OR...
      sessions {
        filter malicious|benign;
        sort-by SHA256|Create Time|Src IP|Src Port|Dst Ip|Dst Port|File|Device
ID|App|Malicious|Status;
        sort-direction asc|desc;
        limit 1-20000;
        days 1-7;
      }
      OR...
      samples {
        filter malicious|benign;
        sort-by SHA256|Create Time|File Name|File Type|File Size|Malicious|Status;
        sort-direction asc|desc;
        limit 1-20000;
        days 1-7;
      }
      OR...
      uploads {
        sort-by SHA256|Create Time|Finish Time|Status;
        sort-direction asc|desc;
        limit 1-20000;
        days 1-7;
      }
    OR...
    last-device-registration {
      all;
    }
  }
```

Opciones

```
admin@wf-corp1> show wildfire
> last-device-registration   Show list of latest registration activities
> latest                     Show latest 30 activities, which include the last 30 analysis activities, the last
                             30 files that were analyzed, network session information on files that were
                             analyzed and files that were uploaded to the public cloud server.
> sample-status              Show wildfire sample status. Enter the SHA or MD5 value of the file to view the
                             current analysis status.
> statistics                 Show basic wildfire statistics
> status                     status
> vm-images                  Shows the attributes of the install virtual machine images used in sample analysis.
                             To view the current active image, run the command show wildfire status and view the
                             Select VM: field. To change the active VM image, from configuration mode, run the
                             command set deviceconfig setting wildfire active-vm and select an image.
```

Resultado de muestra

A continuación se muestra el resultado de este comando.

```
admin@wf-corp1> show wildfire last-device-registration all

+--------------+--------------------+-------------+------------+----------+----
----+
| Device ID    | Last Registered    | Device IP   | SW Version | HW Model | Sta
tus |
+--------------+--------------------+-------------+------------+----------+----
----+
| 001606000114 | 2013-03-12 08:34:09 | 192.168.2.1 | 5.0.2      | PA-200   | OK
    |
+--------------+--------------------+-------------+------------+----------+----

admin@wf-corp1> show wildfire latest
> analysis   Show latest 30 analysis
> samples    Show latest 30 samples
> sessions   Show latest 30 sessions
> uploads    Show latest 30 uploads

show wildfire sample-status sha256 equal
c08ec3f922e26b92dac959f672ed7df2734ad7840cd40dd72db72d9c9827b6e8

Sample information:
+---------------------+------------------+----------+----------+----------+-------
------------+
| Create Time         | File Name        | File Type | File Size | Malicious | Status
|
+---------------------+------------------+----------+----------+----------+-------
------------+
| 2013-03-07 10:22:00 | 5138e1fa13a66.exe | PE       | 261420    | No        | analysis
complete |
| 2013-03-07 10:22:00 | 5138e1fa13a66.exe | PE       | 261420    | No        | analysis
complete |
+---------------------+------------------+----------+----------+----------+-------
------------+
```

```
Session information:
+--------------------+---------------+---------+-------------+---------+---------
----------+-------------+-------------+----------+-----------+
| Create Time        | Src IP        | Src Port | Dst IP      | Dst Port | File
| Device ID     | App           | Malicious | Status     |
+--------------------+---------------+---------+-------------+---------+---------
----------+-------------+-------------+----------+-----------+
| 2013-03-07 10:22:42 | 46.165.211.184 | 80      | 192.168.2.10 | 53620    |
5138e223a1069.exe | 001606000114 | web-browsing | No         | completed |
| 2013-03-07 10:22:02 | 46.165.211.184 | 80      | 192.168.2.10 | 53618    |
5138e1fb3e5fb.exe | 001606000114 | web-browsing | No         | completed |
| 2013-03-07 10:22:00 | 46.165.211.184 | 80      | 192.168.2.10 | 53617    |
5138e1fa13a66.exe | 001606000114 | web-browsing | No         | completed |
+--------------------+---------------+---------+-------------+---------+---------
----------+-------------+-------------+----------+-----------+

Analysis information:
+--------------------+--------------------+--------------------+----------+-------
----+
| Submit Time         | Start Time          | Finish Time         | Malicious | Status
|
+--------------------+--------------------+--------------------+----------+-------
----+
| 2013-03-07 10:22:01 | 2013-03-07 10:22:01 | 2013-03-07 10:27:02 | No         |
completed |
+--------------------+--------------------+--------------------+----------+-------
----+

admin@wf-corp1> show wildfire statistics days 7

Last one hour statistics:
Total sessions submitted  :          0
Samples submitted         :          0
Samples analyzed          :          0
Samples pending           :          0
Samples (malicious)       :          0
Samples (benign)          :          0
Samples (error)           :          0
Malware sent to cloud     :          0

Last 7 days statistics:
Total sessions submitted  :         23
Samples submitted         :          3
Samples analyzed          :          3
Samples pending           :          0
Samples (malicious)       :          0
Samples (benign)          :          3
Samples (error)           :          0
Malware sent to cloud     :          0

admin@wf-corp1> show wildfire status

Connection info:
```

```
        Wildfire cloud:               wildfire-public-cloud
        Status:                       Idle
        Auto-Submit:                  disabled
        VM internet connection:       disabled
        Best server:
        Device registered:            no
        Service route IP address:     192.168.2.20
        Signature verification:       enable
        Server selection:             enable
        Through a proxy:              no
```

Nivel de privilegios requerido

`superuser, superreader`

show system raid

Descripción

Muestra la configuración RAID del dispositivo. El dispositivo WF-500 WildFire se entrega con cuatro unidades en las cuatro primeras bahías de unidades (A1, A2, B1, B2). Las unidades A1 y A2 son el par RAID 1 y las unidades B1 y B2 son el segundo par RAID 1.

Ubicación de jerarquía

`show system`

Sintaxis

```
raid{
        detail;
```

Opciones

No hay opciones adicionales.

Resultado de muestra

A continuación se muestra la configuración RAID en un dispositivo WildFire WF-500.

```
admin@wf-corp1> show system raid detail
```

```
Disk Pair A                         Available
   Status                               clean
   Disk id A1                         Present
       model        : ST91000640NS
       size         : 953869 MB
       partition_1  : active sync
       partition_2  : active sync
   Disk id A2                         Present
       model        : ST91000640NS
       size         : 953869 MB
       partition_1  : active sync
       partition_2  : active sync
Disk Pair B                         Available
   Status                               clean
   Disk id B1                         Present
       model        : ST91000640NS
       size         : 953869 MB
       partition_1  : active sync
       partition_2  : active sync
   Disk id B2                         Present
       model        : ST91000640NS
       size         : 953869 MB
       partition_1  : active sync
       partition_2  : active sync
```

Nivel de privilegios requerido

superuser, superreader